OIC-CERT
Computer Emergency Response Team

OIC-CERT 2025
ANNUAL REPORT

Organization of the Islamic Cooperation
Computer Emergency Response Team

The OIC-CERT Annual Report 2025
provides a comprehensive overview of the activities, achievements, and collaborative efforts undertaken by country members throughout the year 2025. It serves as a valuable platform for sharing progress, highlighting impactful initiatives, and fostering mutual learning across regions. In addition to reflecting on the accomplishments of the past year, this report outlines the planned activities for 2026, offering insights into future priorities and strategic directions. Through this collective documentation, we aim to strengthen regional cooperation and promote continuous improvement in our shared goals.

TABLE OF CONTENT

ABOUT OIC-CERT

The Organization of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT) – www.oic-cert.org was established through the Organization of the Islamic Cooperation (OIC) Resolution No 3/35-INF Collaboration of Computer Emergency Response Team (CERT) Among the OIC Member Countries. It was passed during the 35th Session of the Council of Foreign Ministers of the OIC in Kampala Uganda on 18-20 June 2008

In 2009 through the Resolution No 2/36-INF Granting the Organization of the Islamic Cooperation – Computer Emergency Response Team an Affiliated Institution Status, the OIC-CERT became an affiliate institution of the OIC during the 36th Session of the Council of Foreign Ministers of the OIC Meeting in Damascus, Syrian Arab Republic on 23-25 May 2009

Vision

Envisioning the OIC-CERT to be a leading cybersecurity platform to make the global cyber-space safe

Mission

A platform to develop cybersecurity capabilities to mitigate cyber threats by leveraging on global collaboration

Objectives

- Strengthening the relationship of CERTs among the OIC Member countries, OIC-CERT partners, and other stakeholders in the OIC community
- Encouraging the sharing of cybersecurity experience and information
- Preventing and reducing cyber-crimes by harmonizing cybersecurity policies, laws, and regulations
- Building cybersecurity capabilities and awareness amongst the OIC-CERT member countries
- Promoting collaborative research, development, and innovation in cybersecurity
- Promoting international cooperation with international cybersecurity organizations
- Assisting the OIC-CERT member countries in establishing and developing national CERTs

Membership

As of Jan 2026, the OIC-CERT has a network and strategic collaboration with 69 members from 31 OIC countries. This alliance is further supported through the presence of seven (7) Commercial Members, four (4) Professional Members, four (4) Fellow Member, two (2) Affiliate Member, and 1 Honorary Member

Full Members

These are CERTs, Computer Security Incident Response Teams (CSIRTs) or similar entities that are located and/ or having the primary function within the jurisdiction of the OIC-CERT member countries that is wholly or partly owned by the government with the authority to represent the country's interest

1. **Azerbaijan**
   Azerbaijan Government CERT (CERT.GOV.AZ)
2. **Bahrain**
   National Cyber Security Center (NSCS)
3. **Bangladesh**
   Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)
4. **Brunei Darussalam**
   Brunei Computer Emergency Response Team (BruCERT)
5. **Cote D'Ivoire**
   Cote D'Ivoire Computer Emergency Response Team (CI-CERT)
6. **Egypt**
   Egypt Computer Emergency Response Team (EG-CERT)
7. **Indonesia**
   National Cyber and Cryto Agency (NCCA)
8. **Iran**
   Iran Computer Emergency Response Team (IRCERT)
9. **Jordan**
   Jordan Computer Emergency Response Team (JO-CERT)
10. **Kazakhstan**
    Kazakhstan Computer Emergency Response Team (KZ-CERT)
11. **Kuwait**
    Kuwait National Cyber Security Center (NCSC-KW)
12. **Kyrgyzstan**
    Computer Emergency Response Team of Kyrgyz Republic (CERT-KG)
13. **Libya**
    Libyan Computer Emergency Response Team (Libya-CERT)
14. **Malaysia**
    CyberSecurity Malaysia
15. **Morocco**
    Moroccan Computer Emergency Response Team (maCERT)
16. **Nigeria**
    Consultancy Support Service Limited (CS2)
17. **Oman**
    Oman National Computer Emergency Response Team (OCERT)
18. **Pakistan**
    National Response Centre for Cyber Crimes (NR3C)
19. **Palestine**
    Palestine Computer Emergency Response Team / Government Security Operations Center (PALCERT/ GOV-SOC)
20. **Qatar**
    Qatar Computer Emergency Response Team (Q-CERT)

21. Saudi Arabia
    Saudi Arabia Computer Emergency Response Team (CERT-SA)
22. Somalia
    Somalia Computer Emergency Response Team (SomCERT)
23. Sudan
    Sudan Computer Emergency Response Team (SudanCERT)
24. Syria
    Computer Security Incident Response Team CSIRT of Syria
25. The Gambia
    The Gambia Computer Security and Incident Response Team (gmCSIRT)
26. Tunisia
    National Agency for Computer Security (tunCERT)
27. Türkiye
    National Cyber Security Incident Response Team (TR-CERT)
28. United Arab Emirates
    UAE Computer Emergency Response Team (aeCERT)
29. Uzbekistan
    Uzbekistan Computer Emergency Response Team (UzCERT)

General Members

These are other related government organizations, non- governmental organizations or academia that deals with cybersecurity matters. However, these parties do not have the authority to represent the country's interest

Azerbaijan

1. Azerbaijan Cybersecurity Organizations Association (ACOA)
2. Cyber Security Service (CERT.AZ)

Bangladesh

3. BangladeshCERT
4. Bangladesh Computer Emergency Response Team (bdCERT)

Egypt

5. EG-Financial CIRT (Eg-FinCIRT)

Iran

6. Isfahan University of Technology Computer Emergency Response Team (IUTcert)
7. Amirkabir University of Technology Computer Emergency Response Team (AUTcert)
8. Sharif University of Technology Computer Emergency Response Team (SharifCert)
9. Shiraz University ICT Center (SUcert)
10. Maher Center
11. APA Ferdowsi University of Mashhad CERT (APA-FUMcert)
12. APA University Bojnord CERT (APA-UBCERT)

Jordan

13. Unit of Financial Computer Emergency Response Team (JoFin-CERT)

Kazakhstan

14. 14. Center for Analysis and Investigation of Cyber-Attacks (CAICA)

Kyrgyzstan

15. Computer Emergency Response Team (CERT.ICT KG)
16. Cybersecurity Center of Ala-Too International University (CSC AIU)

Lebanon

17. Leb CSIRT

Malaysia

18. Universiti Teknikal Malaysia Melaka (UTeM)

Pakistan

19. Pakistan Information Security Association (PISA-CERT)

Türkiye

20. Turkey Cyber Security Incident Response Team (TR-CSIRT)

Uganda

21. Uganda Computer Emergency Response Team (UG-CERT)

Uzbekistan

22. Inha University in Tashkent

Affiliate Members

These are not-for-profit organizations that deals with cybersecurity matters from non OIC member countries

1. Team Cymru, United States
2. Ethio-CERT, Ethiopia

Commercial Members

These are industrial or business organizations that deals with cybersecurity matters from the OIC and non-OIC member countries

Brunei Darussalam

1. ITPSS Sdn. Bhd

Bahrain

2. CTM360

Singapore

3. CERT-GIB

Türkiye

4. Turkcell CDC
5. Turkish Airlines CERT (THY-CERT)

Russia

6. Positive Technologies

UAE

7. Huawei (HWT)

Professional Members

Individual experts in information security area providing expert advice pertaining to the collaboration of the OIC-CERT and information security related matters

Malaysia

1. Abdul Fattah Mohamed Yatim - Teknimuda (M) Sdn Bhd
2. Hatim Mohammad Tahir
3. Prof. Dr. Rabiah Ahmad - Universiti Tun Hussein Onn Malaysia

Yemen

4. Dr. Abdulrahman Ahmad Abdul Muthana - Smart Security Solutions

Fellow Members

These are individual who are considered as co-founders of the OIC-CERT and have actively represent their organization as an OIC-CERT member for a minimum period of 5 years

Tunisia

1. Prof. Nabil Sahli

Malaysia

2. Assoc. Prof. Colonel (R) Dato' Ts. Dr. Husin Bin Jazri
3. Ts. Dr. Zahri Yunos
4. Ts. Mohd Shamir Hashim

Honorary Members

Individuals or organizations who has demonstrated extraordinary contribution, support, and exemplary leadership to the OIC-CERT

Saudi Arabia

1. Organisation of the Islamic Cooperation

The OIC-CERT Annual Report is an avenue for members to share their activities and achievements for the year

Board members
(Term: 2024-2028)

Oman	The Oman National Computer Emergency Readiness Team (OCERT), Sultanate of Oman *(Chair)*
Indonesia	National Cyber and Crypto Agency (NCCA), Indonesia *(Deputy Chair)*
UAE	Cybersecurity Council/ The United Arab Emirates - Computer Emergency Response Team (aeCERT), United Arab Emirates *(Deputy Chair)*
Malaysia	CyberSecurity Malaysia, Malaysia *(Permanent Secretariat)*
Azerbaijan	Azerbaijan Government CERT (CERT.GOV.AZ) Republic of Azerbaijan
Brunei	Cyber Security Brunei (CSB), Brunei Darussalam
Egypt	Egyptian Computer Emergency Readiness Team (EgICERT), Egypt
Morocco	Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), Morocco
Qatar	National Cyber Security Agency (NCSA), Qatar
Uzbekistan	SUE "Cybersecurity Center/Uzbekistan Computer Emergency Response Team (UzCERT), Republic of Uzbekistan

OIC-CERT Permanent Secretariat

CyberSecurity Malaysia
Level 7 Tower 1 Menara Cyber Axis
Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA
secretariat@oic-cert.org

Full & General Members

AZERBAIJAN

AZERBAIJAN GOVERNMENT CERT (CERT.GOV.AZ)

HIGHLIGHTS OF 2025

Achievements

- Continued the "Information Security Calendar 2025" project to support consistent security routines and deepen practical awareness across state institutions;
- Published 3 editions of the "Information Security" journals for government bodies;
- Launch of a "bug bounty" reward program in partnership with Qarabug LLC;
- Identified 850 specific cyberattack indicators and blocked on the "AzStateNet" network and email system;
- Shared a total of 1,140 fake URLs on the "Blacklist" platform based on threat information collected from various feed services;
- Prevented the activities of 40 spear phishing campaigns across the country;
- Blocked 449,385,000 malicious links through the new generation security equipment implemented on the "AzStateNet" network, and 96,794 malicious electronic documents through its "Sandbox" protection system;
- Completed the "Tusi Paleon - forensics tool" project by the Malware Research Labaratory of the Center and developed a prototype by defining the initial technical requirements of the new "10C Hunter" project;
- Published a threat research-type articles on the official website of MRLab;
- Trainings on "Best Practices in Cyber Hygiene" and "Digital Security" held at the Ministry of Energy of the Republic of Azerbaijan;
- Prevented a total of 6,205,200 malicious activities through the centralized antivirus system installed on end users of the government entities;
- Identified and centrally blocked 1,302 indicators (1,144 IPs,158 domains) as a result of manual threat investigations;
- Investigated leaked credential data belonging to a total of 137 employees across government entities in relation to various incidents;
- Blocked 75 fake domains impersonating government domains (gov.az);
- Received 1,225 requests/tickets, categorized under 10 classification types, over the "Electronic Request System" from the relevant government entities regarding critical-severity cyber incidents;
- Completed the "Solurius" project – Security Awareness and Training (SAT) & Learning Management System (LMS) developed by Cybersign and passed initial testing;

- Establishing "Malware Analysis" and "Information Security Testing" laboratories at AzTU and BHOS, within the framework of MoUs signed with two educational universities;
- Information security masterclasses held at Baku Higher Oil School (BHOS), Baku Business University and Azerbaijan Technical University (AzTU);
- Initiated development of the OIC-CERT Membership Platform from scratch and fulfilled many technical requirements within a short period;

ABOUT ORGANIZATION

Introduction

Azerbaijan Government CERT (CERT.GOV.AZ) functions under the Special Communication and Information Security State Service of the Republic of Azerbaijan, and offers assistance in computer and network security incident handling and provides 24/7 basis security monitoring and incident coordination functions for all incidents involving systems and networks located in the local state sector.

RFC-2350 – https://cert.gov.az/en/page/rfc-2350
Promo – https://www.youtube.com/watch?v=tYqPc-lzd54

Establishment

2008-04-20

Resources

Official web sites:
- https://cert.gov.az/
- https://scis.gov.az/

Social media links:
- https://youtube.com/@certgovaz
- https://facebook.com/certgovaz
- https://x.com/certgovaz
- https://telegram.me/certgovaz
- https://linkedin.com/company/certgovaz

Constituency

All networks and the users allocated in the state sector of the Republic of Azerbaijan

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- The First Cyber Diplomacy Training at the Twinning Center (17 Mar 2025, Baku, Azerbaijan);
- The 6th Summit Meeting of Heads of State Bodies on Information Security (5 Sep 2025, Baku, Azerbaijan);
- Critical Infrastructure Defense Challenge 2025 (CIDC-2025)(9–10 Oct 2025, Baku, Azerbaijan);
- "Hack The Future 2" training program within CIDC-2025 (9–10 Oct 2025, Baku, Azerbaijan)

- International "Women in Cyber" Conference within CIDC-2025 (11 Oct 2025, Azerbaijan);
- International webinar on "Cyber Diplomacy" for OIC-CERT member countries (3 Nov 2025, Online);
- The 7th Summit Meeting of Heads of State Bodies on Information Security (23 Dec 2025, Nakhchivan, Azerbaijan).

Events involvement

- Bucharest Digital Innovation Summit (8–11 Apr 2025, Bucharest, Romania);
- Youth Cybersecurity Forum 2025 (23 Apr 2025, Baku, Azerbaijan);
- "FDC Summit 2025" event and the Board of Directors meetings of the OIC-CERT organization (28–30 Apr 2025, Cairo, Egypt);
- Gulf Information Security Expo & Conference (GISEC) Global 2025 (6-8 May 2025, Dubai, United Arab Emirates);
- 17th International Conference on Cyber Conflict (CyCon 2025) (27–30 May 2025, Tallinn, Estonia);
- Regional Cybersecurity Week 2025 / Regional Cybersecurity Summit 2025 (15–19 Sep 2025, Rabat, Morocco);
- Annual meeting of the OIC-CERT Board Members (17 Sep 2025, Rabat, Morocco);
- KazHackStan 2025 / "CyberKumbez" competition (22 Sep 2025, Almaty, Kazakhstan);
- "Innovation and Artificial Intelligence" Conference organized by AmCham Azerbaijan (2 Oct 2025, Baku, Azerbaijan).

2026 PLANNED ACTIVITIES

- Continuation the "Information Security Calendar – 2026" project to strengthen information security habits and awareness;
- Continuation to Cyber Hygiene project which will refer to all government employees and accelerating awareness activities;
- Organization of meetings with CISOs of the state institutions on a semi-annual basis;
- Organization of trainings on Cyber Diplomacy;
- Release of the "10C Hunter" project, developed by the Malware Research Laboratory, which performs scanning and detection of IOCs on endpoints over the corporate network;
- Publish the OIC-CERT Membership Portal and continue its development;
- Continue to regular issues of Information Security journals;
- Continue collaboration with CERTs internationally.

The First Cyber Diplomacy Training at the Twinning Center (17 Mar 2025, Baku, Azerbaijan)

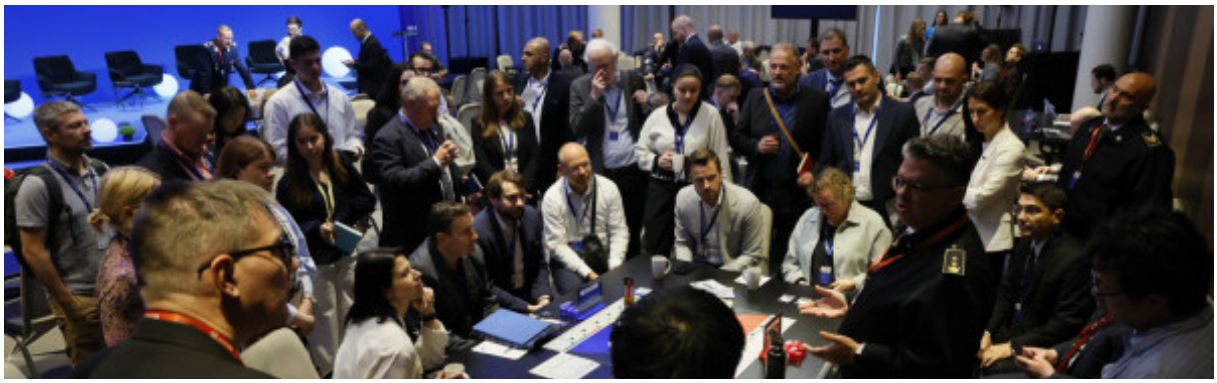
Bucharest Digital Innovation Summit (8–11 Apr 2025, Bucharest, Romania);

Youth Cybersecurity Forum 2025 (23 Apr 2025, Baku, Azerbaijan)

The OIC-CERT Board Members meeting within the "FDC Summit 2025" event (28–30 Apr 2025, Cairo, Egypt)

Gulf Information Security Expo & Conference (GISEC) Global 2025 (6-8 May 2025, Dubai, United Arab Emirates);

17th International Conference on Cyber Conflict (CyCon 2025) (27–30 May 2025, Tallinn, Estonia)



The 6th Summit of IT Heads of State Institutions (5 Sep 2025, Baku, Azerbaijan)

Regional Cybersecurity Week 2025 / Regional Cybersecurity Summit 2025 (15–19 Sep 2025, Rabat, Morocco);

Annual meeting of the OIC-CERT Board Members (17 Sep 2025, Rabat, Morocco)

KazHackStan 2025 / "CyberKumbez" competition (22 Sep 2025, Almaty, Kazakhstan)

"Innovation and Artificial Intelligence" Conference organized by AmCham Azerbaijan (2 Oct 2025, Baku, Azerbaijan)

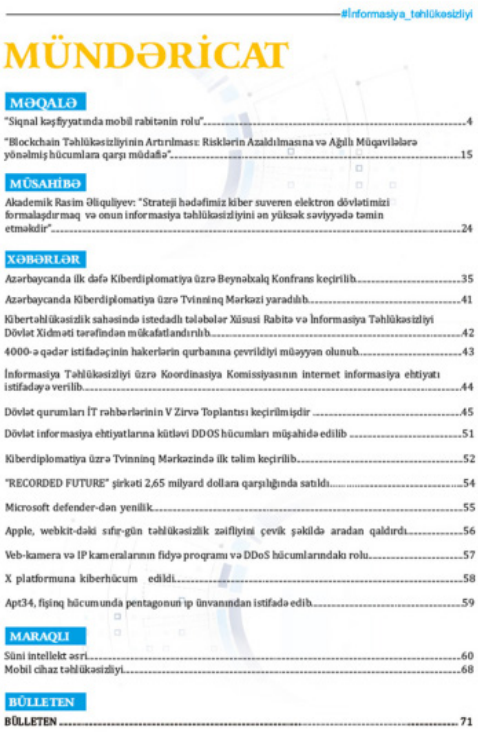
Critical Infrastructure Defense Challenge 2025 (CIDC-2025) (9–10 Oct 2025, Baku, Azerbaijan)

International "Women in Cyber" Conference within CIDC-2025 (11 Oct 2025, Azerbaijan)

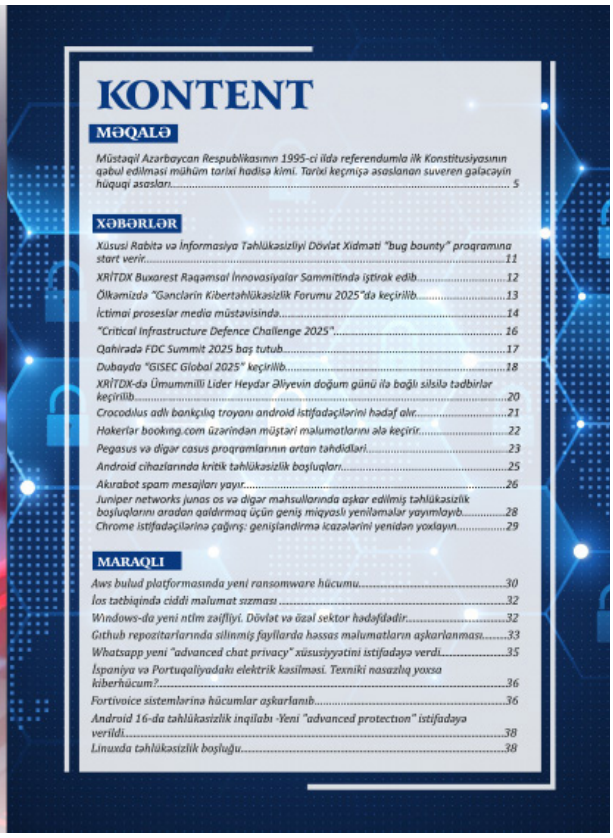
The 7th Summit Meeting of Heads of State Bodies on Information Security (23 Dec 2025, Nakhchivan, Azerbaijan)

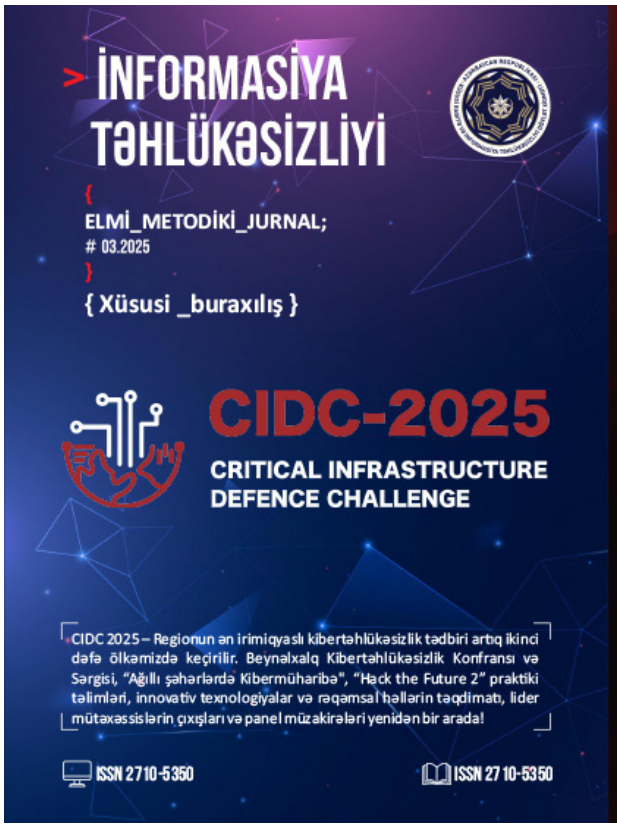
Information security masterclasses at Baku Higher Oil School, Baku Business University and Azerbaijan Technical University

Information Security journals published in 2025 (https://scis.gov.az/en/journal)




>İNFORMASİYA TƏHLÜKƏSİZLİYİ
{
ELMİ_METODİKİ_JURNAL
02,2025/26
}
ISSN 2710-5350
ISSN 2710-5350
JURNAL 11 İYUN 2014-CÜ İL TARİXİNDƏ AZƏRBAYCAN RESPUBLİKASININ ƏDLİYYƏ NAZİRLİYİNDƏ QEYDİYYATDAN KEÇMİŞDİR.
QEYDİYYAT NÖMRƏSİ: 3891


KONTENT
MƏQALƏ
Müstəqil Azərbaycan Respublikasının 1995-ci ildə referendumla ilk Konstitusiyasının qəbul edilməsi mühüm tarixi hadisə kimi. Tarixi keçmişə əsaslanan suveren gələcəyin hüquqi əsasları 5
XƏBƏRLƏR
Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti "bug bounty" proqramına start verir 11
XRİTDX Buxarest Rəqəmsal İnnovasiyalar Sammitində iştirak edib 12
Ölkəmizdə "Gənclərin Kibertəhlükəsizlik Forumu 2025"də keçirilib 13
İctimai proseslər media müstəvisində 14
"Critical Infrastructure Defence Challenge 2025" 16
Qahirədə FDC Summit 2025 baş tutub 17
Dubayda "GISEC Global 2025" keçirilib 18
XRİTDX-də Ümummilli Lider Heydər Əliyevin doğum günü ilə bağlı silsilə tədbirlər keçirilib 20
Crocodilus adlı bankçılıq troyanı android istifadəçilərini hədəf alır 21
Hakerlər booking.com üzərindən müştəri məlumatlarını ələ keçirir 22
Pegasus və digər casus proqramlarının artan təhdidləri 23
Android cihazlarında kritik təhlükəsizlik boşluqları 25
Akırabot spam mesajları yayır 26
Juniper networks junos os və digər məhsullarında aşkar edilmiş təhlükəsizlik boşluqlarını aradan qaldırmaq üçün geniş miqyaslı yeniləmələr yayımlayıb 28
Chrome istifadəçilərinə çağırış: genişləndirmə icazələrini yenidən yoxlayın 29
MARAQLI
Aws bulud platformasında yeni ransomware hücumu 30
İos tətbiqində ciddi məlumat sızması 32
Windows-da yeni ntlm zəifliyi. Dövlət və özəl sektor hədəfdədir 32
Github repozitarlarında silinmiş fayllarda həssas məlumatların aşkarlanması 33
Whatsapp yeni "advanced chat privacy" xüsusiyyətini istifadəyə verdi 35
İspaniya və Portuqaliyadakı elektrik kəsilməsi. Texniki nasazlıq yoxsa kiberhücum? 36
Fortivoice sistemlərinə hücumlar aşkarlanıb 36
Android 16-da təhlükəsizlik inqilabı -Yeni "advanced protection" istifadəyə verildi 38
Linuxda təhlükəsizlik boşluğu 38


>İNFORMASİYA TƏHLÜKƏSİZLİYİ
{
ELMİ_METODİKİ_JURNAL;
# 03.2025
}
{ Xüsusi _buraxılış }
CIDC-2025
CRITICAL INFRASTRUCTURE DEFENCE CHALLENGE
CIDC 2025 – Regionun ən irimiqyaslı kibertəhlükəsizlik tədbiri artıq ikinci dəfə ölkəmizdə keçirilir. Beynəlxalq Kibertəhlükəsizlik Konfransı və Sərgisi, "Ağıllı şəhərlərdə Kibermüharibə", "Hack the Future 2" praktiki təlimləri, innovativ texnologiyalar və rəqəmsal həllərin təqdimatı, lider mütəxəssislərin çıxışları və panel müzakirələri yenidən bir arada!
ISSN 2710-5350
ISSN 2710-5350


CIDC-2025
CRITICAL INFRASTRUCTURE DEFENCE CHALLENGE
BAKI KONQRES MƏRKƏZİ
9-10 OKTYABR 2025-Cİ İL

AZERBAIJAN

ELECTRONIC SECURITY SERVICE UNDER THE MINISTRY OF DIGITAL DEVELOPMENT AND TRANSPORT

MINISTRY OF DIGITAL DEVELOPMENT AND TRANSPORT
ELECTRONIC SECURITY SERVICE

HIGHLIGHTS OF 2025

Summary of Major Activities

- According to the National Cyber Security Index (NCSI) as of January 2026, Azerbaijan scored 75.83 points and ranked 48th, demonstrating continuous progress in cybersecurity preparedness.
- To strengthen internal coordination and ensure a unified approach to incident management, a dedicated system (MISP) has been implemented. Through this system, incident registration, case management, and forensic classification have been organized in a more structured manner, significantly enhancing operational efficiency.
- Within the framework of international cooperation, partnerships with National CERTs of various countries and leading technology companies have been expanded, and proof-of-concept (PoC) projects on advanced cybersecurity solutions have been implemented.
- ESS has actively participated in international cybersecurity initiatives, contributed to global knowledge exchange, and supported the strengthening of the country's international cybersecurity standing.

Achievements

- Throughout 2025, significant improvements were achieved in the coordination of the national cybersecurity domain, resulting in more structured, systematic, and effective information exchange among institutions.
- Cooperation with international organizations and partners has been expanded, and the exchange of technical knowledge and expertise has been strengthened.

ABOUT ORGANIZATION

Electronic Security Center (ESC) under the Ministry of Digital Development and Transport (MDDT) was established pursuant to the 5th part of the Decree of the President of the Republic of Azerbaijan № 708, dated September 26, 2012. By the Decree of the President of the Republic of Azerbaijan on additional measures to improve management in transport, communications and

high technologies field, dated January 12, 2018, the Center was included in the structure of the Ministry of Digital Development and Transport as the Electronic Security Service (ESS). The ESS serves as a coordinating state authority responsible for overseeing the activities of entities within the information infrastructure. It promotes awareness-raising of existing and potential e-dangers at the national level, provides education on cybersecurity for the citizens, private entities, and organizations, and offers methodological assistance to enhance cybersecurity practices. The Service conducts its activities in accordance with national legislation, state programs, and the national cybersecurity strategy.

ACTIVITIES & OPERATION

Scope and definitions

- The activities carried out by ESS cover the monitoring, analysis, and coordination of cybersecurity incidents, as well as the strengthening of the security of information systems within the private sector.
- Upon request, reviews are conducted regarding incidents and vulnerabilities identified in the information systems of state institutions, with methodological and technical recommendations provided and support ensured for incident management processes.
- Relevant measures have been undertaken in line with the implementation of the "Information Security and Cybersecurity Strategy of the Republic of Azerbaijan for 2023–2027".

Incident handling reports

- During the reporting period, cybersecurity incident management activities were carried out based on requests received from public and private sector entities. Within this framework, technical and analytical assessments were conducted to determine the nature, scale, and potential impact of incidents, and structured recommendations were provided to support their effective management.
- The exchange of national cybersecurity threat intelligence has been enhanced, and the number of institutions integrated into the MISP (Malware Information Sharing Platform) system increased in 2025, significantly improving coordinated response capabilities.
- Organizations affected by cyberattacks such as DDoS, phishing, ransomware, and data breaches were provided with recommendations to address vulnerabilities in their information resources and to implement preventive measures.

Abuse statistics

Throughout the reporting period, cybersecurity-related statistical data were systematically collected, processed, and analyzed to identify trends, patterns, and emerging risks within the national cyber environment. These statistics provide valuable insights for strategic planning and prioritization of cybersecurity measures.

- A total of 329,650 botnet-related incidents were recorded and continuously monitored throughout the year;
- 187 phishing incidents were identified, with associated risks to users and organizations assessed;
- 1,386 DDoS attacks were detected and analyzed;
- Malware distribution incidents reached 359,167 cases;
- During the reporting period, the total number of cyberattacks targeting network devices amounted to 333,756;
- Web-based attacks totaled 2,003,995 incidents;
- Ransomware attacks accounted for 29,517 cases during the reporting period.

Publication(s)

An article by the ESS representative on "A Preliminary Analysis of Operational Challenges in Cyber Threat Intelligence" was published in OIC-CERT Journal of Cyber Security Volume 6 in 2025.

New service(s)

- During the reporting period, ESS continued its efforts to enhance cybersecurity capabilities through the implementation of advanced technological solutions and the expansion of existing systems.
- To evaluate the effectiveness of cyber defense controls, existing protection mechanisms were tested through the emulation of real-world attack scenarios.
- In addition, the application of artificial intelligence-based approaches was analyzed, particularly with regard to risk modeling and prioritization capabilities.
- Furthermore, pilot implementations of advanced solutions based on international best practices were carried out, and their integration potential into the national cybersecurity environment was assessed.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

ESS held an awareness-raising event for employees of "Azergold" CJSC to form a culture of information security and cybersecurity and ensure cyber hygiene on January 16, 2025.

Educational events were held at 10 secondary schools, jointly organized by ESS and the "Friend of the Schoolchild" project in January and March, 2025. The aim of the events was to educate schoolchildren in the field of cybersecurity, inform them about cyber hygiene rules and safety rules in the online environment. More than 1100 schoolchildren participated in the training.

ESS employees spoke on Azerbaijan Television's (AzTV) Medialab program on January 21, 2025. During the speech, they discussed the types of social engineering attacks and methods of protection against them.
https://youtu.be/3JT-PhfXR_Q?si=GsZKfihE3tw-tb2h

Within the framework of the joint cooperation between the ESS and 21st Century International Education and Innovation Center, an educational event dedicated to the "International Safer Internet Day" was organized on February 11, 2025. At the event attended by 50 people, parents were provided with extensive information on the protection of personal data, rules for using social media, combating cyberbullying, and password security.
https://www.instagram.com/reel/DF7D1tcNvVF/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

ESS delivered a speech on the topic of "Protecting Children from Harmful Information" via live broadcast on the Facebook page of the State Committee for Family, Women and Children Affairs on February 11, 2025.
https://www.instagram.com/reel/DRjouswCOmf/?igsh=MWxoeWZxYjltZzg0

Educational events were held by ESS at Azerbaijan Technical University on March 12, 2025. In total, 200 students attended the event, and ESS staff gave speeches on the topics of "Cybersecurity in the Online Environment" and "Fundamentals of Cybersecurity". The aim of the event was to educate students on the topics of information security and cybersecurity in higher education institutions, as well as the use of social networks.
https://www.instagram.com/reel/DHLmpdPIiL1/?utm_source=ig_web_copy_link

On April 10, 2025, the Deputy Head of the ESS spoke on the "QabuldASAN" program about the activities of Service, as well as the most widespread cyber threats of recent times.
https://www.instagram.com/asantv.az/reel/DIOT1qOoQWu/

"Youth Cybersecurity Forum-2025" was held with the support of the ESS, Youth Foundation, the Special Communication and Information Security State Service, and the Azerbaijan Cybersecurity Center, and was organized by the Union of Student Youth Organizations of Azerbaijan on April 23, 2025. Within the framework of the event, ESS participated in panel discussions on the topics "Artificial Intelligence and the Human Factor: New Changes in Cybersecurity and the Risks We Face" and "Cybersecurity: New Approaches in Programming and Data Protection."

On April 25, 2025, an educational event for students was organized by ESS on the occasion of the International "Girls in ICT Day". The event was attended by 33 young girls studying at the Azerbaijan State Oil and Industry University (ASOIU), as well as the Azerbaijan-French University (UFAZ). ESS provided information to students about the professional activities of the entity in the field of information security and ways to resolve real cyber incidents, and answered their questions.
https://www.instagram.com/etx.azerbaijan/reel/DI3LJs1Ikg7/

ESS was invited to participate in the "Economic Zone" program On April 25, 2025. During the interview, an ESS provided useful information about cyber fraud cases occurring in the country and methods of protection against them.
https://www.instagram.com/etx.azerbaijan/reel/DI_Qr0yoecU/

On May 2, ESS participated in the panel session on "Safe digital media environment: informed users" held within the framework of the II Forum "Social processes in the media sphere" organized by the Media Development Agency.

During the panel discussion, ESS exchanged extensive views on the complex impacts of technological evolution on the media environment, the protection of reliable information, the role of social media as a source of information, the risks of cyberattacks, and the possibilities of effective communication through digital tools.

On May 14, a training on cybersecurity was held for representatives of media entities in partnership with the ESS, the Innovation and Digital Development Agency (IDDA), the Media Development Agency, and "AzInTelecom" LLC, which operates within the Azerbaijan Transport and Communication Holding (AZCON Holding). The representative of the ESS management delivered an opening speech at the event.

An educational event on cybersecurity was organized by the joint initiative of ESS and AccessBank on May 23, 2025. The event was held for AccessBank employees and parents of customers, as well as members of the "Third Spring" Public Union.

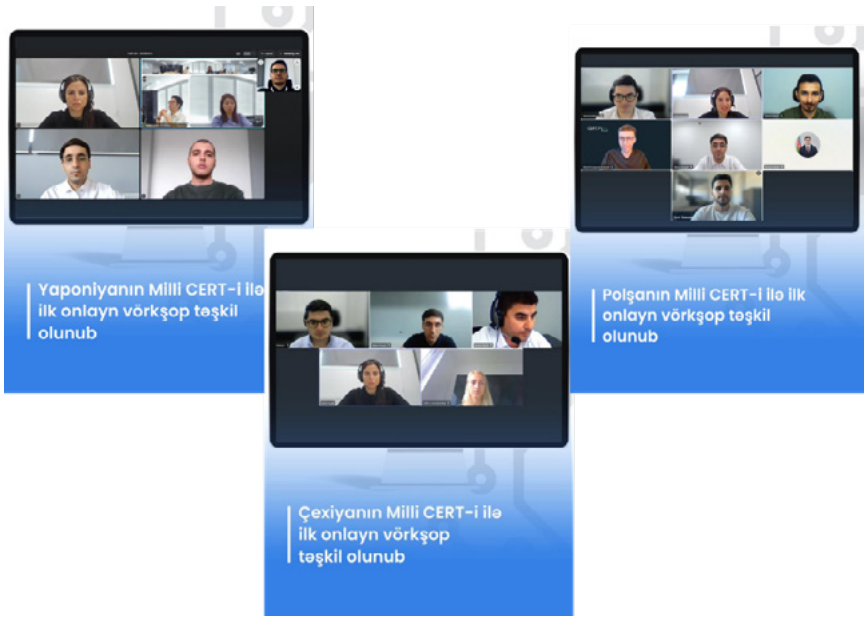
On May 30, 2025, ESS participated in the scientific-practical conference held on the topic of "Development and strategic cooperation in the protection of children's rights" with the initiative of the Ministry of Internal Affairs of the Republic of Azerbaijan. ESS staff member spoke about the importance of protecting children's rights in the digital environment, preventive approaches to online dangers and threats, taking preventive measures against harmful content, as well as effective and coordinated cooperation between government agencies in this direction.

On June 4, ESS participated in the roundtable organized by the State Committee for Family, Women and Children Affairs on the topic of "Protection of Children in the Cyber Environment and Joint Action Against Digital Threats." During the discussions, the importance of strengthening the protection of children in the online environment at a time when digital threats are increasing was emphasized. The importance of coordinated action by government agencies, media representatives, and civil society in this direction was noted.

On June 12, 2025, the first online workshop on "Cybersecurity Awareness Activities" was organized between ESS and the National Cybersecurity Center (NCSC-FI) under the Finnish Transport and Communications Agency. The main goal of the workshop was to share best practices in cybersecurity awareness, establish effective communication, and strengthen cooperation between the two institutions.

The "Cybersecurity Seminar for Leaders" series was held at the initiative of the Azerbaijan Cybersecurity Center (ACC) in partnership with ESS. The seminar was attended by the leaders responsible for cybersecurity and information security from about 20 state institutions. Leading experts from the "Technion" Institute of Technology delivered presentations covering current cybersecurity challenges and best practices. The experts shared their experiences on national cyber defense systems, preventive strategies against the most common malware and hacker attacks, and other critical topics, as well as exchanged views with leading representatives of government agencies.

In August and September 2025, online workshops on "Cybersecurity Awareness Activities" and "Cybersecurity Information Exchange" were organized between ESS and the National CERT of Japan (JPCERT/CC), the National CERT of the Czech Republic (CSIRT.CZ), and the National CERT of the Republic of Poland (CERT.PL). The main purpose of the workshops was to conduct detailed discussions on the work carried out by the institutions in the field of cybersecurity and cybersecurity awareness, the measures taken against cyber attacks, and the methods used to raise awareness among citizens and organizations about cyber threats. Within the framework of the workshops, the parties made detailed presentations on the directions of their activities in the field of cybersecurity, awareness-raising programs, and the security measures they implemented.



On October 6, 2025, ESS participated in the training "Protecting Children from Harmful Information", contributing to discussions and exchanging views on efforts to strengthen children's online safety and promote digital literacy.
https://www.cert.az/news/2025/etx-aqupdk-tedbir

As of October 15, educational videos have been shared on the institution's social networks as part of the "ETX Educates" project.
https://www.instagram.com/reel/DP07oi5CC7G/?utm_source=ig_web_button_share_sheet

On October 16, 2025, a training on cybersecurity was held for representatives of member states of the Conference on Interaction and Confidence-Building Measures in Asia (CICA) organized by the Ministry of Digital Development and Transport, the Innovation and Digital Development Agency, and ESS. Along with local and international experts, ESS specialists also spoke at the training and shared their views on current challenges and advanced solutions in the field of cybersecurity. During the training, presentations were shown to participants on topics such as modern cyber threats, incident management, critical infrastructure protection, and information security.

A meeting was held between the Central Bank of the Republic of Azerbaijan (CBA) and the ESS on strengthening cooperation on information security and cybersecurity in the financial sector.

Within the framework of the cooperation, the parties agreed to work together to ensure coordinated activities in the field of information security and cybersecurity in the sector, organize relevant events, as well as provide mutual information on incidents, cyberattacks and other threats.

A Memorandum of Understanding was signed online between ESS and CyberSecurity Malaysia on October 30, 2025. The document is of great importance in terms of expanding strategic partnership in the field of information security and cybersecurity, as well as strengthening mutual support in regional and global initiatives.

A meeting was held at the ESS as part of the visit to Azerbaijan of a delegation led by the Deputy Minister of Artificial Intelligence and Digital Development of Kazakhstan, Doszhan Musaliyev. During the meeting, views were exchanged on cooperation opportunities.

In collaboration with the Committee on Family, Women and Children's Issues, educational video instructions for parents were prepared and published for a wide audience on various social media platforms.
https://www.instagram.com/etx.azerbaijan/reel/DRjpUaZiE6o/
https://www.instagram.com/etx.azerbaijan/reel/DRjpBHTCPTB/
https://www.instagram.com/etx.azerbaijan/reel/DRjouswCOmf/

A representative of the ESS participated in the international conference organized by the State Committee for Family, Women and Children Affairs on the topic "Protection of children in the digital environment: Modern tools and international cooperation." Within the framework of the conference, at the panel on the topic "Threats in the digital environment: Solutions and modern approaches", ESS representative spoke about the main cyber threats faced by children in the digital environment, ways to prevent these risks, and educational approaches.

Educational visuals and information have been and continue to be presented in Azerpocht parcels, DOST Centers, and ASAN Service branches. In addition, educational information on cybersecurity is being sent to approximately 4 million users within the framework of cooperation with the "SIMA" digital platform.
https://www.instagram.com/etx.azerbaijan/reel/DRMoK1tiEDV/
https://www.instagram.com/etx.azerbaijan/reel/DRylGRaCJg-/

On November 25-26, 2025, ESS participated in the seminar on "Artificial Intelligence in Cybersecurity" held by NATO and organized by the Ministry of Foreign Affairs of the Republic of Azerbaijan. The ESS representative spoke about the role of artificial intelligence technologies in the operational detection and prevention of malicious programs, information operations and other cyber threats.
https://www.cert.az/news/2025/etx-kibertehlukesizlik-tedbir

Events involvement

ESS participated in the training course on "Cybercrime Investigations" held in Doha, Qatar, from 23-27 February 2025.

ESS participated in the GISEC Global 2025 and ITU Global CyberDrill 2025 events held in Dubai, UAE, from 5-8 May 2025

ESS participated in the Cybersecurity Alliance for Mutual Progress (CAMP) 10th Anniversary Celebration & Annual Meeting held in Seoul, South Korea, from 8-10 July 2025.

ESS participated in the OIC-CERT 17th Annual Conference held in Rabat, Morocco, from 15-19 September 2025.

ESS participated in the "KazHackStan 2025" event held in Almaty, Kazakhstan, from 17-19 September 2025.

ESS participated in the Cyber Security Summit for Central Eurasia held in Tashkent, Uzbekistan, from 7-8 October 2025.

On October 8, 2025, within the framework of participation in the "Cyber Security Summit 2025" held in Tashkent, Republic of Uzbekistan, a Memorandum of Understanding was signed between the ESS and the State Unitary Enterprise "Cybersecurity Center" of the Republic of Uzbekistan.

ESS participated in the international training on "Integrated Cybersecurity for a Safer Digital World" held in the Republic of Singapore, from 13-17 October 2025.

ESS visited the headquarters of the Information Technology and Communications Authority, as well as the Personal Data Protection Authority of the Republic of Türkiye from 26-27 November. Cooperation between entities, as well as future opportunities for collaboration were discussed during the meetings. Additionally, an exchange of views was held on the approaches adopted by both countries in the areas of cybersecurity, digital stability, and data protection.

2026 PLANNED ACTIVITIES

- To ensure a unified approach to the classification of cyber threats at the national level, it is planned to enhance the legal framework, develop relevant regulatory acts, and ensure their formal adoption.
- In order to strengthen the national cybersecurity ecosystem, it is planned to expand Threat Intelligence capabilities and reinforce their implementation at the national level.
- The development of the Security Operations Center (SOC) infrastructure is envisaged to ensure effective monitoring and operational management of security incidents.
- It is planned to further expand activities related to the adoption of advanced cybersecurity technologies, the enhancement of existing systems, and the integration of innovative solutions.

CONCLUSION

As a result of the activities carried out during the reporting period, institutional, technological, and operational capabilities in the field of cybersecurity have been strengthened across the country. The measures implemented in line with the national cybersecurity strategy have contributed to effective risk management and the improvement of the regulatory and legal framework.

BANGLADESH

BGD E-GOV CIRT

BGD e-GOV CIRT

HIGHLIGHTS OF 2025

Summary of Major Activities

- BGD e-GOV CIRT has successfully organized "Cyber Drill 2025 for Critical Information Infrastructure & Financial Institutions"
- Cyber Threat Intelligence" unit published 240 Cyber Threat Alerts and 17 Cyber Threat Advisories/Alerts.
- VAPT conducted on 566 servers and network devices, along with 40 web applications, mobile app, and API applications across 17 engagements involving 11 unique organizations.
- 37 cyber sensor analysis reports have been provided to multiple Critical Information Infrastructures.
- Digital forensic services provided to eleven (11) organizations, with 20 artifacts analyzed across thirteen (13) cases.
- Risk-based IT audits have become a cornerstone of the national cybersecurity strategy in Bangladesh. These assessments systematically conducted across various sectors including Critical Information Infrastructures and government organizations.
- Provided Cyber security training to 113 Govt. officials in 2025

Achievements

- Provided technical support for the design and deployment of cyber drill artifacts for the Agile Cyber Drill 2025.
- Delivered technical assistance in organizing and conducting a Capture The Flag (CTF) competition for the PKI Hackathon under the Controller of Certifying Authorities (CCA).
- Provided technical support for the design and deployment of cyber drill artifacts for the MIST Cyber Drill 2025.

ABOUT ORGANIZATION

Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) currently acts as the National CERT of Bangladesh (N-CERT), with responsibilities including receiving, reviewing, and responding to computer security incidents and activities. Under the Government of the People's Republic of Bangladesh, BGD e-GOV CIRT reviews and takes necessary measures to resolve issues with broad cybersecurity implications, conducts research and development, and provides guidance on security vulnerabilities. BGD e-GOV CIRT also collaborates with various government units, Critical Information Infrastructures, financial organizations, law enforcement agencies, academia, and civil society to strengthen Bangladesh's cybersecurity defenses.

The process to establish BGD e-GOV CIRT began in November 2014, and the team started operations in February 2016. Currently, 17 people are working at BGD e-GOV CIRT.

Its constituency includes all governmental, semi-governmental, and autonomous bodies, ministries, and institutions of Bangladesh. BGD e-GOV CIRT currently operates as the National CERT of Bangladesh with a mandate to serve the entire country.

ACTIVITIES & OPERATION

Scope and definitions

BGD e-GOV CIRT serves as the primary technical authority for securing Bangladesh's government digital infrastructure. We lead national efforts to build cyber resilience and establish robust incident management capabilities across all critical sectors.

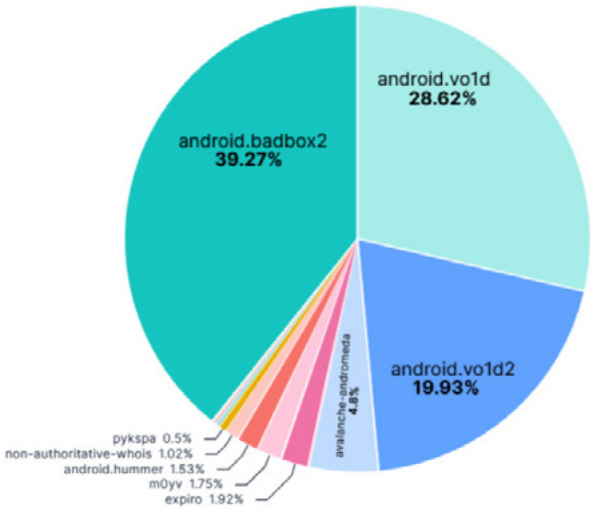
Incident handling reports

BGD e-GOV CIRT responded and investigated 7 major cyber incidents for different sectors of Bangladesh

Abuse statistics

In 2025, the Cyber Threat Intelligence (CTI) unit of BGD e-GOV CIRT identified 107 unique malware strains from internet traffic specific to Bangladesh. The top five malware infections based on detected cases were:

- Android.bandbox2
- Android.Vo1d
- Android.Vo1d2
- Avalanche-Andromeda
- Expiro
- M0yv
- Android.Hummer



Publication(s)

A Cyber Threat Landscape report for Bangladesh has been published

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- Conducted Training on Cyber Incident Response at National Cyber Security Agency (NCSA) for Twenty Government officials.
- Provided Advance Digital Forensics training to Law Enforcement Agency and Government officials at DoICT.
- Workshop on 'Software and Tools Used in Cybersecurity' at Bangladesh Computer Council.
- Cybersecurity training for the Department of Disaster Management on Practical OSINT for Threat Hunting.
- Provided hands-on training about cyber sensor activities to Military Institute of Science and Technology (MIST) students as part of their Industrial Attachment program.
- Training program on cyber threat analysis, detection, and mitigation for Law Enforcement Agency.
- Provided Basic Cyber Security training to Government officials at the Ministry of Law.
- Provided Cyber Range Management training to different university academicians.

Events involvement

- Participated in the APCERT Cyber Drill 2025.
- Attended the OIC 13th Regional Cyber Drill 2025.
- Participated in the ITU Global Cyber Drill 2025.
- Attended the "JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region (FY2025).

2026 PLANNED ACTIVITIES

- Organize and conduct cybersecurity drills across various sectors to test, evaluate,
- and enhance the readiness of organizations in responding to cyber incidents.
- Perform systematic Vulnerability Assessment and Penetration Testing (VAPT) across diverse sectors to identify and remediate security gaps.
- Conduct risk-based IT audits of Critical Information Infrastructure (CIIs)
- Provide regular cyber sensor analysis report (Intrusion, Suspicious activity) to Critical Information Infrastructure where Cyber sensor deployed.
- Conduct ICS and cybersecurity training for government and public sector organizations to enhance skills and preparedness.

CONCLUSION

In an era of rapidly evolving cyber threats, BGD e-GOV CIRT continues to prioritize proactive defense, robust incident management, and strong collaboration across all sectors. Over the past year, the team has focused on reinforcing critical infrastructure, improving real-time threat detection, expanding intelligence sharing, and enhancing the skills of cybersecurity personnel. Looking ahead, BGD e-GOV CIRT remains dedicated to advancing technological capabilities, strengthening workforce expertise, and fostering partnerships across government, industry, and academia to ensure a resilient and secure digital environment for Bangladesh.

Figure 1: Cyber Drill 2025 for Critical Information Infrastructure & Financial Institutions Host Team

Figure 2: Cyber Drill 2025 for Critical Information Infrastructure & Financial Institutions Participants

Figure 3: Workshop on 'Software and Tools Used in Cybersecurity

Figure 4: Workshop on 'Software and Tools Used in Cybersecurity

Figure 5: ITU Global Cyber Drill 2025

Figure 6: Training program on cyber threat analysis, detection, and mitigation for Law Enforcement Agency.

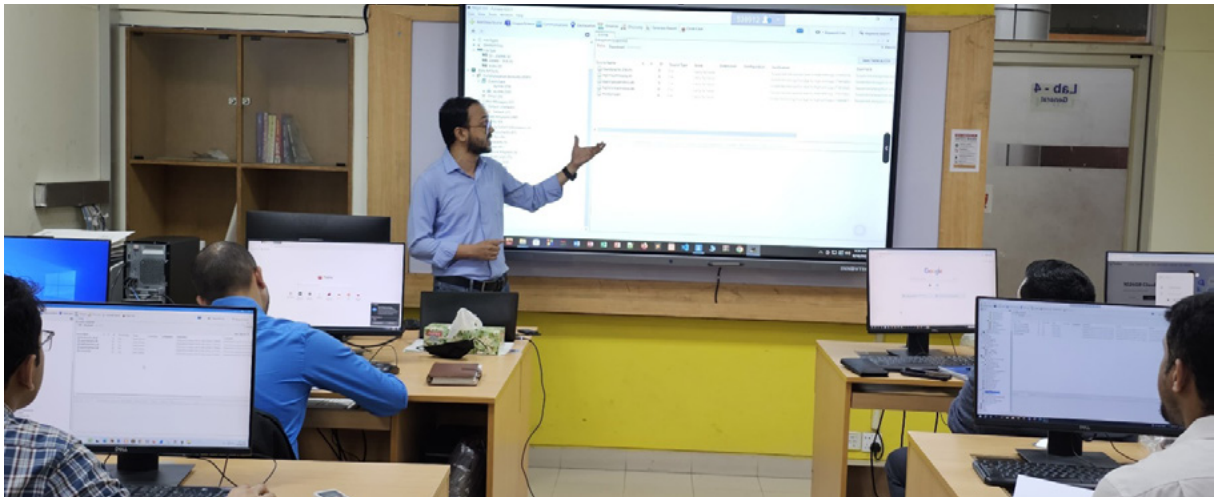


Figure 7: Advance Digital Forensics training to Law Enforcement Agency and Government officials.

BRUNEI DARUSSALAM

BRUCERT

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

ABOUT ORGANIZATION

Introduction

Cyber Security Brunei (CSB) is the national cybersecurity agency of Negara Brunei Darussalam, responsible for safeguarding the nation's cyberspace and coordinating national efforts to address cybersecurity threats and cybercrime. CSB operates under the Ministry of Transport and Infocommunications (MTIC), with the Minister of MTIC serving as the Minister-in-Charge of Cybersecurity.

CSB plays a key role in strengthening the country's cybersecurity posture by providing services and initiatives that support government agencies, private sector organisations, and the general public. These efforts focus on protecting Critical Information Infrastructure (CII), enhancing national cyber incident response capabilities, supporting cybercrime investigations through the National Digital Forensics Laboratory (NDFL), and promoting cybersecurity awareness across the nation.

BruCERT (Brunei Computer Emergency Response Team) was established in May 2004 as Brunei Darussalam's national incident response team. Originally formed in collaboration with the Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) and the then Ministry of Communications, BruCERT serves as the country's trusted focal point for handling computer-related and internet-related security incidents. Today, BruCERT operates under Cyber Security Brunei and provides incident response coordination, cybersecurity advisory, and threat analysis services.

Supporting these operations is the Cyber Watch Centre (CWC), which functions as the national cybersecurity monitoring and situational awareness center. CWC conducts continuous monitoring of cyber threats affecting government systems and Critical Information Infrastructure (CII) through advanced security monitoring technologies, intelligent sensors, and threat intelligence capabilities. The center plays a crucial role in detecting potential cyber threats, analysing malicious activities, and providing early warning alerts to strengthen national cyber defence.

BruCERT actively collaborates with regional and international cybersecurity communities to enhance information sharing, technical cooperation, and coordinated incident response. The team is a member of several global cybersecurity organisations, including:

- Asia Pacific Computer Emergency Response Team (APCERT) – joined in 2005
- Organisation of Islamic Cooperation Computer Emergency Response Team (OIC-CERT) – joined in 2009
- Forum of Incident Response and Security Teams (FIRST) – joined in 2014

Through these collaborations, CSB, BruCERT, and the Cyber Watch Centre continue to strengthen Brunei Darussalam's national cyber resilience, incident response capabilities, and international cybersecurity cooperation.

BruCERT Services

- 24X7 Security Related Incidents and Emergency Response from BruCERT.
- 24X7 Security Related Incidents and Emergency Response onsite (Deployment response is within 2hrs after an incident is received). This service only applies to BruCERT Constituents.
- Broadcast alerts (Early Warning) of new vulnerabilities, advisories, viruses and Security Guidelines from BruCERT Website. BruCERT Constituents will receive alerts through email and telephone as well as defense strategies in tackling IT Security related issues.
- Promote Security Awareness program to educate and increase public awareness and understanding of information security and technical know-how through education, workshop, seminar, and training.
- Coordinating with other CERT, Network Service Providers, Security Vendors, Government Agencies as well as other related organizations to facilitate the detection, analysis, and prevention of security incidents on the internet.

BruCERT Establishment

BruCERT coordinates with local and international Computer Security Incident Response Team (CSIRTs), Network Service Providers, Security Vendors, Law Enforcement Agencies as well as other related organizations to facilitate the detection, analysis, and prevention of security incidents on the Internet.

BruCERT Workforce

BruCERT currently comprises a workforce of 66 personnel, all of whom are local professionals, reflecting the organisation's commitment to nurturing and strengthening national cybersecurity talent in Brunei Darussalam. The majority of the team consists of highly skilled information technology and cybersecurity specialists, supported by personnel responsible for administrative and technical operations.

To ensure operational excellence and readiness in addressing the evolving cyber threat landscape, BruCERT continuously invests in the professional development and technical capacity building

of its workforce. Staff members have undergone extensive training across a broad spectrum of information technology and cybersecurity disciplines, supported by internationally recognised professional certifications.

These include industry certifications such as CompTIA A+, Network+, Linux+, Server+, and Security+, as well as advanced cybersecurity certifications including SCNP, SCNA, CIW, CEH, CCNA, CISSP, and ISO/IEC 27001 Implementer.

In addition, BruCERT personnel have participated in specialized training programmes offered by the SANS Institute, including GREM (Reverse Engineering Malware), GCIA (Intrusion Analysis), GCIH (Incident Handling), GCFA (Forensic Analysis), and GPEN (Penetration Testing). Many members of the team have successfully obtained these certifications, further strengthening BruCERT's capabilities in incident response, malware analysis, digital forensics, threat intelligence, and cybersecurity operations.

Through continuous professional development and skills enhancement, BruCERT remains committed to building a highly capable and resilient cybersecurity workforce, enabling the organisation to effectively safeguard the digital ecosystem and support the national cybersecurity mission of Brunei Darussalam.

BruCERT Constituents

BruCERT has close relationships with Government agencies, 1 major ISPs and various numbers of vendors.

Government Ministries and Departments
BruCERT provide Security incident response, Managed Security Services via Cyber Watch Centre (CWC) and Consultancy services to the government agencies. Security Trainings such as forensic and awareness trainings were provided by BruCERT in collaboration with some Government Agencies.

E-Government National Centre (EGNC)
E-Government National Centre provides IT Services to all Government Departments and Ministries in Brunei Darussalam. Services such as IT Central procurement, Network Central Procurement, Co-location, ONEPASS (a PKI initiative), Co-hosting are provided by EGNC. BruCERT works closely with EGNC in providing Incident Response and Security Monitoring since most of the government equipment resided at EGNC.

AITI

Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) is an independent statutory body to regulate, license and develop the local ICT industry and manage the national radio frequency spectrum.

AITI has appointed ITPSS (Information Technology Protective Security Services), an IT local security company to become the national CERT in dealing with incident response in Brunei.

Royal Brunei Police Force (RBPF) and other Law-Enforcement Agencies (LEAs)
BruCERT has been collaborating with RBPF and other LEAs to resolve computer-related incidents through our Digital and Mobile Forensic services.

Unified National Network – UNN
UNN, the main Internet service provider. BruCERT have been working together to engage information sharing of internet-related statistics and the current situation of IT environment in Brunei.

Brunei Cyber Security Association – BCSA
Brunei Cyber Security Association (BCSA) aims to. Bring together professionals, experts, and enthusiasts in the field of cybersecurity to collaborate, share knowledge and collectively address the evolving challenges posed by cyber threats.

BruCERT Contact

The Brunei Computer Emergency Response Team Coordination Centre (BruCERT) welcome reports on computer security related incident. Any computer related security incident can be reported to us by:

Telephone: (673) 2458001
Facsimile: (673) 2456211
Whatsapp: (673) 7170766
Email: cert@brucert.org.bn
Reporting: reporting@brucert.org.bn

ACTIVITIES & OPERATION

Incidents response

For the year 2025, Cyber Security Brunei (CSB), through BruCERT and the Cyber Watch Centre (CWC), identified multiple instances of suspicious and malicious activities through its secure monitoring infrastructure and intelligent sensors deployed across constituent systems.

Based on the collected monitoring data, Malware-related incidents accounted for the majority of detected cases, with a total of 1,955 incidents, making it the most prominent cybersecurity concern observed during the year. Malware infections typically indicate attempts by threat actors to compromise systems, establish persistence, or deploy malicious payloads within targeted networks.

Meanwhile, Denial of Service (DoS) incidents recorded only 2 cases, suggesting that large-scale service disruption attempts were relatively minimal compared to other forms of cyber threats observed during the year. The distribution of these detected activities is illustrated in Figure 1.

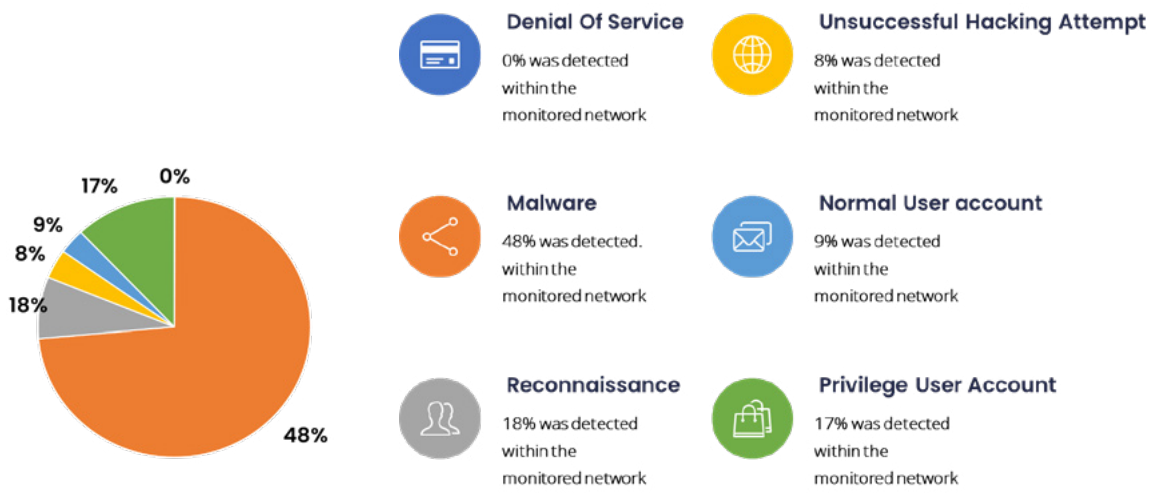


Figure 1

This was followed by Unsuccessful Hacking Attempts (320 cases), which reflect repeated attempts by attackers to gain unauthorized access to systems through methods such as credential brute-force attacks, exploitation of vulnerabilities, or unauthorized login attempts. In addition, Reconnaissance activities (202 cases) were also detected, indicating that attackers were actively probing and scanning systems to gather information about potential vulnerabilities and system configurations before launching further attacks.

The monitoring system also identified several security events related to user account activities, including Normal User Account incidents (97 cases) and Privilege User Account incidents (83 cases). These events highlight potential risks associated with user access management and may indicate suspicious login behavior, privilege misuse, or attempts to escalate system privileges. Overall, the data highlights that malware infections and unauthorized access attempts remain the dominant cybersecurity threats, emphasizing the importance of continuous monitoring, strong access control policies, and proactive threat detection to safeguard critical systems and digital infrastructure in Brunei Darussalam.

Types of Attacks	Count
Denial of Services	1
Malicious Software	504
Reconnaissance	192
Unsuccessful Hacking Attempt	81
Normal User Account	95
Privilege User Account	182

Table 1

BruCERT Honey Pot

Cyber Security Brunei (CSB) through BruCERT has deployed honeypot systems, which are intentionally exposed decoy servers designed to attract and record malicious activities from

cyber attackers. These systems allow BruCERT to observe attacker behaviour, identify commonly targeted services, and analyse emerging cyber threats.

Based on the analysis of logs collected from the honeypot in 2025, it was observed that port 445, commonly associated with Server Message Block (SMB) services, was the most abused port, recording approximately 2,868,603 attack attempts. This indicates a significant number of exploitation attempts targeting SMB-related vulnerabilities, which are commonly used for unauthorised remote access, lateral movement, or malware propagation within networks.

The second most targeted port was port 1433, which is associated with Microsoft SQL Server (MS-SQL) services, with 1,757,603 attempts detected. This suggests that attackers were actively attempting to exploit database services through brute-force login attempts or vulnerability exploitation.

This was followed by port 22 (Secure Shell – SSH) with 989,166 attempts, indicating persistent attempts by attackers to gain remote access to systems through credential brute-forcing or unauthorized login attempts. Other frequently targeted ports included port 23 (Telnet), port 135 (RPC), port 5060 (SIP), port 8728 (MikroTik RouterOS), port 443 (HTTPS), and port 1900 (UPnP), reflecting a broad range of automated scanning and exploitation activities targeting various network services.

Overall, the data demonstrates that attackers continue to focus on commonly exposed services such as SMB, database servers, and remote access protocols, highlighting the importance of proper network hardening, secure configuration, and continuous monitoring to mitigate potential exploitation attempts.

The distribution of the top 10 most abused ports observed by the BruCERT honeypot in 2025 is illustrated in Figure 2.

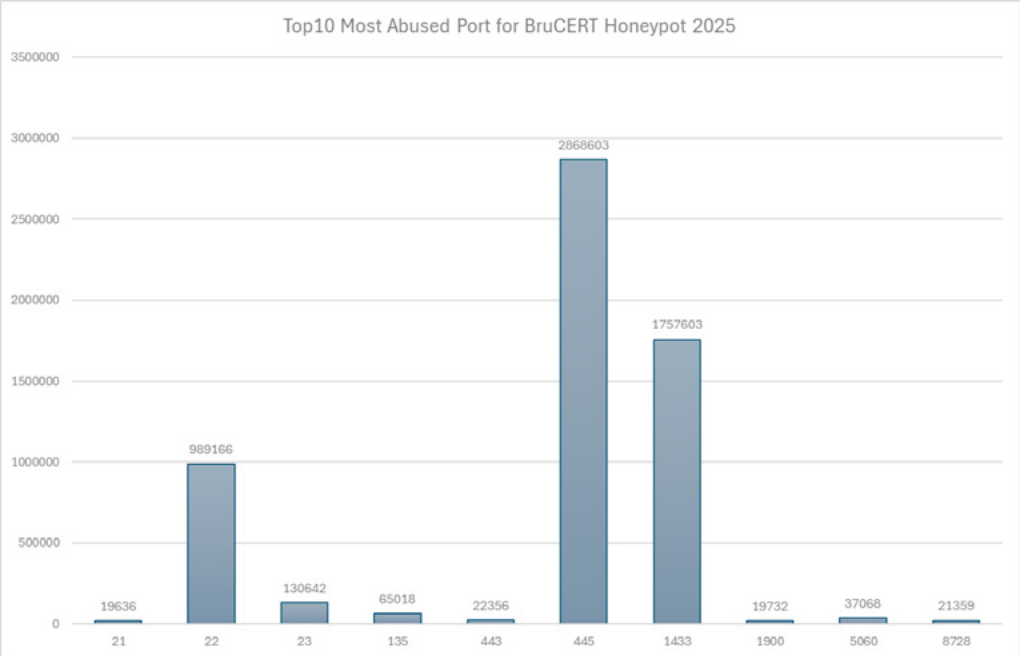


Figure 2

Port No	Count
21	19636
22	989166
23	130642
135	65018
443	22356
445	2868603
1433	1757603
1900	19732
5060	37068
8728	21359

Table 2

Similarly, port 22, which supports Secure Shell (SSH) remote access, recorded 989,166 attempts, highlighting continued efforts by attackers to gain unauthorized administrative access through brute-force login attempts or compromised credentials. The notable activity on port 23 (Telnet), with 130,642 attempts, reflects ongoing exploitation of legacy remote access services that are often poorly secured or misconfigured.

Other ports also demonstrated consistent malicious activity. Port 135 (RPC) recorded 65,018 attempts, suggesting reconnaissance and exploitation targeting Windows remote procedure call services. Port 5060, commonly associated with Session Initiation Protocol (SIP) used in Voice over IP (VoIP) systems, recorded 37,068 attempts, which may indicate attempts to exploit telecommunication infrastructure.

In addition, port 8728, used by MikroTik RouterOS management services, recorded 21,359 attempts, indicating automated scanning targeting network infrastructure devices. Smaller but notable activity was also observed on port 1900 (UPnP) with 19,732 attempts, which could potentially be leveraged for reflection-based DDoS attacks, and port 21 (FTP) with 19,636 attempts, suggesting continued attempts to exploit unsecured file transfer services. Meanwhile, port 443 (HTTPS) recorded 22,356 attempts, which may reflect scanning activities targeting web services and encrypted communication channels.

Overall, the findings highlight that attackers continue to focus on widely deployed and commonly exposed services such as SMB, SSH, and database servers, while also probing legacy services and network infrastructure devices for potential weaknesses. These observations emphasize the importance of secure configuration, regular patching, network segmentation, and continuous monitoring to reduce the risk of exploitation and strengthen the cybersecurity posture of organisations in Brunei Darussalam.

Based on observations from the BruCERT honeypot deployment, several variants of malware were detected attempting to compromise exposed systems. Analysis of the captured samples

indicates that Generic Trojan malware constituted the largest proportion of detected threats, accounting for approximately 53% of the total captured malware. This suggests that attackers frequently deploy Trojan-based payloads to gain unauthorized access, establish persistence, or deliver additional malicious components into targeted systems.

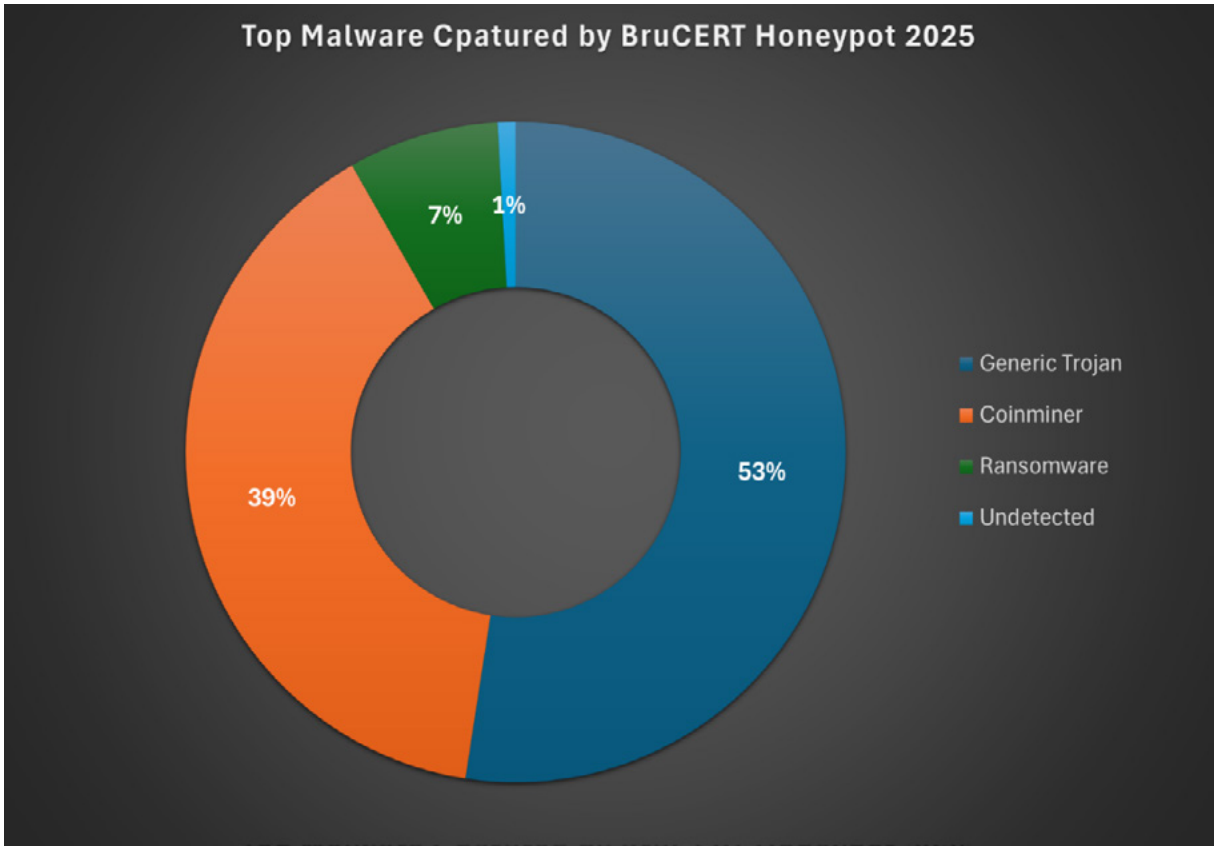


Figure 3

The second most prevalent threat observed was Coinminer malware, representing 39% of the captured samples. Coinminer infections typically aim to exploit compromised systems by utilizing their computational resources for unauthorized cryptocurrency mining, which can significantly degrade system performance and operational stability.

Malware Type	Total
COINMINER	2767
GENERIC TROJAN	3693
RANSOMWARE	520
UNKNOWN	62
Grand Total	**7042**

Table 3

In addition, Ransomware accounted for around 7% of the detected malware, indicating continued attempts by threat actors to deploy ransomware payloads that could potentially encrypt organizational data and disrupt critical services. A small proportion, approximately 1%, remained

undetected or unidentified, reflecting malware samples that could not be immediately classified during the analysis process.

The distribution of malware captured by the honeypot is illustrated in Figure 3, which highlights the dominance of Trojan and cryptocurrency-mining malware in the observed threat landscape. These findings demonstrate the importance of maintaining continuous monitoring mechanisms, such as honeypots, to detect emerging threats and enhance situational awareness of cyberattack patterns targeting networks in Brunei Darussalam.

In 2025, BruCERT recorded a total of 609 reported cybersecurity incidents submitted by the public, government agencies, and private sector organisations in Brunei Darussalam. Analysis of these reports indicates that Phishing incidents constituted the highest number of cases, with 111 reports, followed by Scam-related incidents (91 cases) and Cyberbullying (89 cases).

Other notable incident categories included general cyber-related cases classified as Others (80 cases) and Account Takeover incidents (65 cases), where attackers gained unauthorized access to online accounts. In addition, Impersonation (44 cases), Smishing (37 cases), and Phishing-related variants (35 cases) were also reported, highlighting the continued use of social engineering techniques by cybercriminals.

A smaller number of incidents were recorded under Unethical Communication (18 cases), Sextortion (16 cases), Blackmail or Extortion (16 cases), and Compromised Devices (6 cases). These cases reflect emerging threats that target individuals through harassment, coercion, or unauthorized device access.

Overall, the data demonstrates that social engineering and online fraud remain the dominant cybersecurity threats affecting users in Brunei Darussalam, with phishing and scam-related activities continuing to be the primary methods used by threat actors to exploit victims.

The distribution of reported incidents is illustrated in Figure 4.

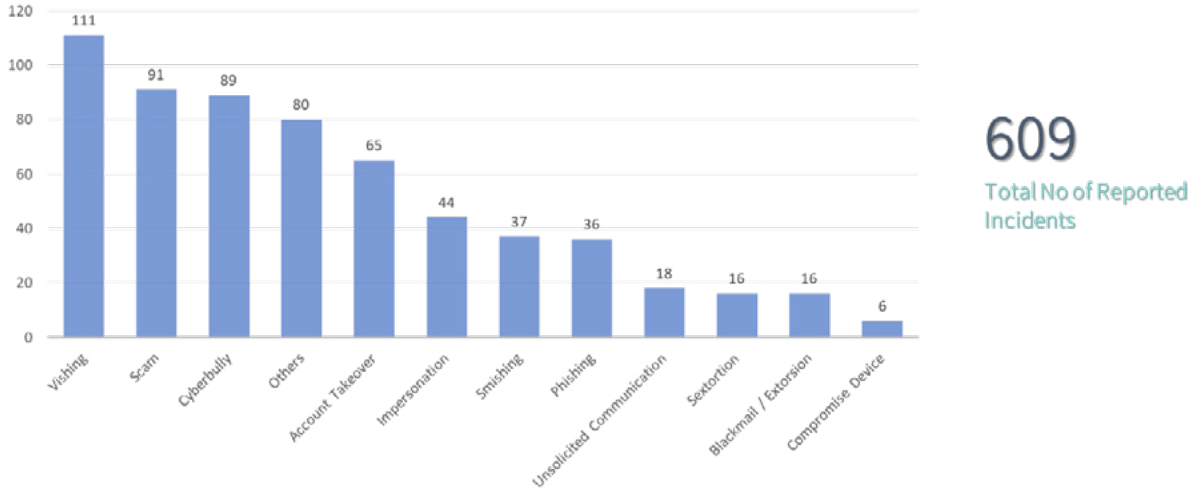


Figure 4

BruCERT Activities in 2025

Seminars/Conferences/Meetings/Visits

In 2025, BruCERT continued to actively participate in various international cybersecurity meetings, conferences, and capacity-building programmes to strengthen collaboration with global Computer Emergency Response Teams (CERTs) and cybersecurity communities. These engagements provided valuable opportunities for information sharing, incident coordination, and discussions on emerging cybersecurity threats and best practices. Several meetings were conducted both physically and through virtual platforms.

- From 25th November 2025 until 27th November 2025 – BruCERT delegates attended the 23rd Annual General Meeting (AGM) and Annual Conference of the Asia Pacific Computer Emergency Response Team (APCERT) hosted by the Australian Cyber Security Centre in Sydney, Australia. The meeting gathered APCERT member teams from across the Asia-Pacific region to discuss regional threat trends, incident response coordination, and strategies to strengthen cybersecurity cooperation among member economies.
- From 15th September 2025 until 16th September 2025 – BruCERT delegates attended the 17th Annual Conference of the Organisation of Islamic Cooperation Computer Emergency Response Team (OIC-CERT). The conference brought together cybersecurity professionals and CERT representatives from OIC member states to discuss regional cyber threats, policy coordination, and collaborative initiatives aimed at enhancing cybersecurity resilience across member countries.
- From April 2025 – BruCERT participated in the APCERT Cyber Drill 2025, a regional cybersecurity exercise organised by APCERT to strengthen incident response capabilities among member teams. The exercise simulated various cyberattack scenarios and allowed participating CERTs to practice information sharing, incident analysis, and coordinated response mechanisms.
- In 2025 – BruCERT participated in the ITU Regional Cyber Drill hosted in Mongolia, organised by the International Telecommunication Union (ITU). Notably, BruCERT contributed its expertise in developing cyber incident scenarios for the exercise, supporting the design of realistic attack simulations used during the drill. The exercise included scenarios such as phishing campaigns, malware infections, and distributed denial-of-service (DDoS) attacks, enabling participating teams to practice coordinated incident response, technical investigation, and cross-border threat intelligence sharing among international CERT communities.

Awareness Activities

Throughout 2025, Cyber Security Brunei (CSB), through BruCERT, continued to strengthen national cybersecurity awareness through a series of public outreach and education initiatives targeting government agencies, organisations, and the public.

A total of 132 awareness sessions were conducted during the year, reaching 15,337 participants

across schools, government institutions, and community groups. These programmes were delivered by seven certified trainers, focusing on key topics such as cyber hygiene, online safety, scam awareness, and emerging cyber threats.

BruCERT's digital awareness platform, www.secureverifyconnect.info, served as a central resource hub for cybersecurity information and recorded an average of 773 visits per month. In addition, BruCERT expanded its outreach through media and digital engagement, including participation in the "Rampai Pagi" radio segment and the production of 111 awareness episodes, with an average of six educational videos played monthly.

Complementing these efforts, 12 structured awareness sessions and targeted engagement programmes were conducted, while 146 users successfully completed the online awareness modules, demonstrating growing public participation in cybersecurity education.

Figure 5

These initiatives reflect BruCERT's continued commitment to enhancing cybersecurity awareness and fostering a safer digital environment across Brunei Darussalam.

In 2025, BruCERT conducted a total of 132 cybersecurity awareness sessions across various sectors in Brunei Darussalam. Most of these sessions were delivered to schools (77 sessions), reflecting a strong focus on educating students and youth on safe digital practices. This was followed by government agencies (38 sessions), community groups (17 sessions), and corporate organisations (7 sessions). These initiatives demonstrate BruCERT's continued efforts to promote cybersecurity awareness and strengthen cyber resilience across multiple segments of society.

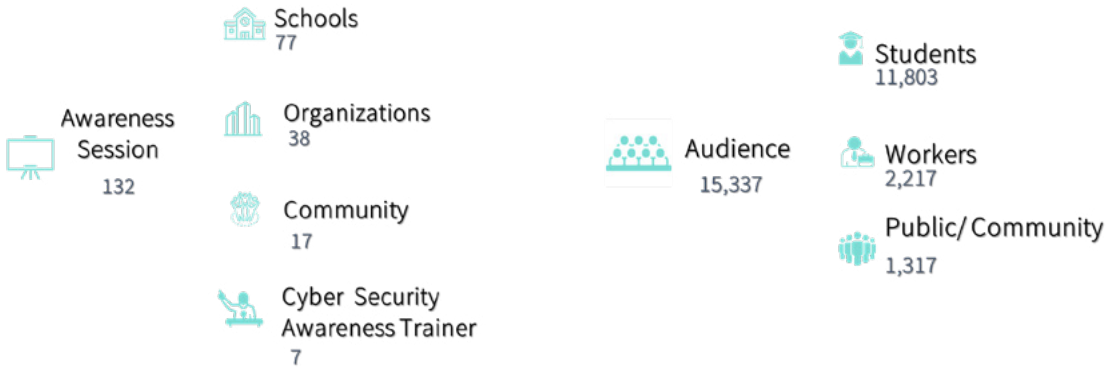


Figure 6

EGYPT

EG | CERT

HIGHLIGHTS OF 2025

Summary of Major Activities

In 2025, the Egyptian Computer Emergency Readiness Team (EG-CERT), operating under the National Telecommunications Regulatory Authority (NTRA), continued to advance its national mandate for cyber incident response, early warning, analysis, and protection of Egypt's communications and critical information infrastructure, alongside structured training delivery. EG-CERT's activities reflected a multidimensional approach combining operational readiness, capacity building, awareness, cybersecurity ecosystem enablement, and international engagement – in line with Egypt's National Cybersecurity Strategy 2023–2027.

Key highlights of 2025 include:

- Operational Excellence: Egypt achieved 1st place globally in the ITU Global CyberDrill 2025, held in the UAE at GISEC 2025 (May 2025).
- Capacity Building & Youth: Organisation of EG-CTF 2025 at CAISEC (May 2025) with 1,656 participants across 635 teams; launch of the 2nd Cybersecurity Academy for Youth targeting 2,000 school students and 1,000 university students across 10 governorates.
- Awareness: Cybersecurity Awareness Month 2025 in collaboration with The American University in Cairo (AUC), including a live attack simulation and "Cyber Space Explorers" sessions.
- Industry Development: Launch of WE Innovate Star (September 2025) and the WE Innovate 2025 Hackathon; "Cybersecurity Industry: Challenges and Opportunities" event on 13 December 2025.
- GRC & Regulatory: Operationalisation of NTRA's Regulatory Framework for Cybersecurity Service Providers, with companies beginning to obtain accreditation under the regime.
- International Cooperation: Egypt's signature of the UN Convention on Countering Cybercrime in Hanoi, October 2025.

Achievements

1st Place – ITU Global CyberDrill 2025: EG-CERT represented Egypt at the ITU Global CyberDrill held in the UAE at GISEC 2025, securing first place internationally among all participating national CIRT teams – demonstrating operational maturity and technical preparedness in international cyber incident response simulation. egcert.eg/news/globalcyberdrill2025/

Figure 1: EG|CERT team wins the 1st place in ITU Global CyberDrill 2025 at GISEC, UAE

UN Cybercrime Convention Signatory: Egypt signed the United Nations Convention on Countering Cybercrime in Hanoi on 25–26 October 2025, linking EG-CERT's work to Egypt's broader international cybercrime cooperation and cross-border response agenda.

EG-CTF 2025 National Competition: Held at CAISEC 2025 (25–26 May 2025) with 1,656 registered participants forming 635 teams. Online qualifiers: 23 May 2025. Prize pool: 1st place EGP 100,000 | 2nd EGP 75,000 | 3rd EGP 50,000. Challenges covered web exploitation, reverse engineering, cryptography, and digital forensics. https://www.facebook.com/MCITEgypt/posts/eg-cert-organizes-second-edition-of-capture-the-flag-national-cybersecurity-comp/1137816695055289/

Figure 2: EG-CTF 2025 National Competition at CAISEC 2025

Cybersecurity Academy for Youth – 2nd Edition: Targeted 2,000 school students (ages 10–17) and 1,000 university students, delivered across 10 governorates via Egypt Digital Creativity Centres. Topics included cybersecurity fundamentals, privacy and data protection, and cyber ethics. https://egcert.eg/news/cybersecurityheroes2025/

Figure 3: Cybersecurity Academy for Youth [2nd Edition]

NTRA Cybersecurity Accreditation Regime – Market Adoption: The NTRA Regulatory Framework for Cybersecurity Services moved into active enforcement during 2025, with firms obtaining full cybersecurity licensingas among the first companies under the regime (October 2025). Covered service categories include penetration testing, red team operations, vulnerability assessment, SOC, incident response, digital forensics, consulting, and training. https://www.tra.gov.eg/ar/%D8%A7%D9%84%D8%B5%D9%86%D8%A7%D8%B9%D8%A9/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A/%D8%A7%D9%84%D8%B4%D8%B1%D9%83%D8%A7%D8%AA-%D8%A7%D9%84%D9%85%D8%B9%D8%AA%D9%85%D8%AF%D8%A9-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A7%D9%8B/.

ABOUT ORGANIZATION

The Egyptian Computer Emergency Readiness Team (EG-CERT) was established by the National Telecommunications Regulatory Authority (NTRA) in April 2009. It provides around-the-clock essential support for protecting critical information infrastructure. Its team comprises highly skilled technical specialists to monitor cybersecurity status, respond to incidents, analyse digital evidence, perform malware analysis, and conduct reverse engineering. Within its mandate, EG-CERT seeks primarily to enhance the security of Egypt's communications and information infrastructure through taking proactive measures, gathering and analysing information on security incidents, coordinating with stakeholders and relevant parties to resolve these incidents, and boosting international cooperation with other Computer Emergency Response Teams (CERTs) around the globe.

The strenuous efforts made by the Cybersecurity Vice-Presidency across its various business units–namely the Egyptian Computer Emergency Readiness Team (EG-CERT), the Governance, Risk and Compliance (GRC) Sector, the Cybersecurity Industry Development Sector, International Bureau for Cybersecurity and Legal Bureau for Cybersecurity–contributed to Egypt's achievement in the most recent edition of the Global Cybersecurity Index (GCI) issued by the International Telecommunication Union (ITU) in September 2024, as it has been recognized as one of the world's top-performing nations. This index classifies countries worldwide in cybersecurity based on their achievements across five pillars: the Legislative Pillar, the Regulatory Pillar, the Technical Pillar, the International Cooperation Pillar, and the Capacity Building Pillar. Egypt scored 100 points, placing it in Tier 1 and among the top countries globally.

ACTIVITIES & OPERATION

Scope and definitions

EG-CERT's operational scope covers national computer and information security incident response, cyber early warning, malware propagation monitoring, and defence of Egypt's telecommunications and critical information infrastructure. Its functions span the full cybersecurity lifecycle: Identify, Protect, Detect, Respond, and Recover.

Incident handling reports

Digital Forensics, Cybercrime Operations & Threat Intelligence – 2025

In 2025, EG-CERT handled 151+ digital forensics cases covering data wiping, cryptocurrency investigations, data extraction, device theft, social media investigations, and cyber intrusion incidents. Six cybercrime cases were detected and referred to competent authorities, and six detailed security warnings on emerging cybercrime patterns were issued and disseminated through EG-CERT's official platforms. To support proactive national threat detection, EG-CERT produced 15 malware analysis reports and 12 threat intelligence reports, alongside 50 threat detection rules to strengthen early warning and risk mitigation capabilities. EG-CERT also coordinated with the Ministry of Transport to secure the electronic interconnection network of the High-Speed Rail project stations, contributing to the protection of critical national digital infrastructure, and supported 17 entities in addressing infrastructure security inquiries.

Abuse statistics

Security Alerts & Early Warning – 2025

EG-CERT monitored critical security updates across operating systems, hardware, software, and applications, issuing 92 detailed security alerts distributed on a regular basis through official channels throughout 2025. Complementing this, the team developed 50 threat detection rules deployed to strengthen national monitoring and automated threat identification capabilities.

Publication(s)

- **Security Alerts**

  EG-CERT continued issuing cybersecurity alerts across its official social media platforms throughout 2025, helping organisations and individuals protect against emerging software vulnerabilities, including 65+ alert count. https://egcert.eg/alerts/

- **Digital Awareness Campaigns**

  Multiple campaigns published covering the 2025 threat landscape, cybercriminal motivations, risk mitigation best practices, and national cybersecurity guidelines. https://egcert.eg/publications/

- **Cybersecurity Awareness Month Content**

  EG-CERT published a dedicated awareness content series throughout October 2025 in collaboration with AUC, including session outputs and post-event highlights on official channels. https://egcert.eg/news/auccybersecuritymonth/

- **EG-CERT launched a dedicated awareness campaign (November 2025)**

  addressing digital violence against women and girls, with a particular focus on cyber blackmail. Implemented as part of the global 16 Days of Activism Against Gender-Based Violence initiative, the campaign aimed to promote preventive measures, raise awareness of women's digital rights, and encourage safe reporting without intimidation.

New service(s)

- **Governance, Risk & Compliance (GRC) Operations – 2025**

  In 2025, EG-CERT strengthened national cybersecurity compliance through a range of regulatory, supervisory, and preventive actions. Key outcomes included: registering 16 companies as cybersecurity service providers and issuing 319 authorisation certificates to 176 individuals, generating total revenues of EGP 8.43 million; certifying 7 cloud service providers out of 15 licensed companies; conducting on-site security assessments for 43 national and critical assets; compiling applications from 79 entities for MCIT and coordinating inventory infrastructure data for cybersecurity assessments; and supporting 17 entities in addressing infrastructure security inquiries.

- **NTRA Cybersecurity Service Provider Accreditation Register**

  The NTRA publicly maintained and updated a dedicated live register of accredited cybersecurity companies and individuals under the 2025 regulatory framework, with a formal channel for registration inquiries available at tra.gov.eg.

- **Regulatory Frameworks for Digital Payment & Cloud Providers**

  EG-CERT prepared cybersecurity regulatory frameworks for the cyber authorisation of mobile-based direct payment service providers, cloud computing service providers, and electronic payment platform operators – advancing governance of Egypt's growing digital financial and cloud infrastructure.

- **WE Innovate Star Programme**

  Launched September 2025 to support national cybersecurity industry development through innovation and entrepreneurship, expanding the WE Innovate ecosystem established in prior years.

- **WE Innovate 2025 Hackathon**

  An open call for students, graduates, entrepreneurs, and innovators to contribute to building national cybersecurity products and solutions.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

EG-CTF 2025 – National Capture The Flag Competition
Organised on the sidelines of CAISEC 2025, Cairo. Online qualifiers: 23 May 2025. Finals: 25–26 May 2025 at Royal Maxim Palace Kempinski, under the patronage of Egypt's Prime Minister. 1,656 participants | 635 teams | Total prize pool: EGP 225,000. Challenge categories: web exploitation, reverse engineering, cryptography, digital forensics.

Cybersecurity Academy for Youth – Summer 2025 (2nd Edition)
Launched in cooperation with Egypt Digital Creativity Centres. Target beneficiaries: 2,000 school students (ages 10–17) and 1,000 university students. Delivered across 10 governorates. Core topics: cybersecurity fundamentals, privacy and data protection, cyber ethics.

Cybersecurity Awareness Month 2025 (October)
Conducted in cooperation with The American University in Cairo (AUC). Launch event: 1 October 2025, featuring cybersecurity sessions across AUC schools supported by private-sector partners. Activities included a live attack simulation and an interactive "Cyber Space Explorers" session. The programme concluded with a public closing announcement in November 2025. https://egcert.eg/news/auccybersecuritymonth/

Figure 4: Cybersecurity Awareness Month 2025 organized by EG|CERT in cooperation with the AUC

Cybersecurity Industry: Challenges and Opportunities Event
Held 13 December 2025, in cooperation with NTRA and hosted with AUC support. Focused on cybersecurity market development, ecosystem constraints, and national opportunity creation.

WE Innovate 2025 Hackathon - (3rd Edition)
Open call for students, graduates, entrepreneurs, and innovators to contribute to building national cybersecurity industries and products under the WE Innovate initiative. https://egcert.eg/ar/news/weinnovatehackathon3/

Figure 5: We Innovate Hackathon [3rd edition]

National Cybersecurity Training Programmes – 2025

In 2025, EG-CERT delivered specialised cybersecurity training under several national programmes, including the Digital Egypt Builders Initiative, the Cybersecurity Academy for Juniors and Youth, and the Youth Telecom Ambassadors Program. Training focused on advanced, practice-oriented areas including digital forensics, incident response, risk management, and secure digital infrastructure.

Cybersecurity Support for Government Agencies – 2025

In 2025, EG-CERT delivered targeted cybersecurity workshops and awareness sessions across key government institutions, combining regulatory implementation support with tailored training to strengthen institutional protection and promote safe digital transformation. Activities included a specialised workshop at the Egyptian Nuclear and Radiological Regulatory Authority on the National Cybersecurity Core Controls (June), awareness lectures at the National Center for Social and Criminological Research covering cybercrime, data protection, and responsible AI use (December), and NTRA-led awareness sessions at the Ministry of Transport and the Ministry of Housing, Utilities and Urban Communities targeting administrative staff on device security, threat prevention, and digital rights (December).

Cooperation Agreement with the Supreme Council of Universities

NTRA/EG-CERT signed a cooperation agreement with the Supreme Council of Universities to embed cybersecurity within Egypt's higher education system. Under the agreement, a Train-the-Trainers programme was delivered for faculty representatives from participating universities, covering cybersecurity fundamentals in preparation for integrating content into the Supreme Council's Digital Transformation Fundamentals Certificate.

Figure 6: Academic & Institutional Capacity Building

Cybersecurity Awareness – University Outreach

EG-CERT delivered cybersecurity awareness sessions at universities including Badr University in Cairo and Fayoum University, targeting students and academic staff on cybersecurity fundamentals, threat awareness, and digital safety practices. The outreach was accompanied by an MOU signed with Badr University for ongoing cybersecurity cooperation.

Figure 7: Cybersecurity Awareness

Train-the-Trainers Programme – Cybersecurity Specialists

EG-CERT implemented a specialised Train-the-Trainers programme delivered with international experts, qualifying Egyptian cybersecurity specialists as certified trainers to build a sustainable national training capacity aligned with the National Cybersecurity Strategy 2023–2027.

Events involvement

ITU Global CyberDrill 2025 – GISEC, UAE (May 2025)
EG-CERT participated in GISEC 2025, the premier global cybersecurity event, represented Egypt and achieved 1st place among all participating international CERT teams. The ITU-organised exercise is designed to strengthen national cyber readiness, improve incident response procedures, and deepen cooperation among national CIRT communities globally.

CAISEC 2025 – Cairo, Egypt (May 2025)
EG-CERT supported and participated in the Cyber and Information Security Exhibition and Conference (CAISEC 2025), Egypt's premier national cybersecurity conference, where EG-CTF 2025 finals were also held under the patronage of the Prime Minister.

UN Cybercrime Convention Signing Ceremony – Hanoi, Vietnam (25–26 October 2025)
Egypt, represented by Minister of Communications and Information Technology Dr. Amr Talaat, signed the United Nations Convention on Countering Cybercrime. EG-CERT/NTRA was among the negotiating bodies and publicly linked this milestone to Egypt's international cyber cooperation agenda. https://see.news/egypt-signs-un-convention-on-combating-cybercrime

EVENTS ORGANIZED & INVOLVEMENT2026 PLANNED ACTIVITIES

Advancement of National Cyber Resilience and Critical Infrastructure Protection
EG-CERT will continue to enhance national early warning and incident response capabilities, expanding its role as the central technical coordination hub for cyber incident management. This includes:

- Deployment of advanced threat detection platforms leveraging AI and large-scale analytics.
- Expansion of sector-specific monitoring capabilities for critical information infrastructure, including energy, finance, and smart city systems.
- Strengthening national cyber crisis management and large-scale simulation exercises.

This direction is consistent with the national mandate to provide early warning, incident analysis, and coordinated response across Egypt's critical ICT infrastructure.

Capacity Building and National Workforce Development
A core pillar of future activities will focus on scaling human capital through:

- National training initiatives such as cybersecurity academies and youth programs.
- Professional certification pathways and specialized technical training.
- Regional capacity-building programs targeting African and OIC member states.

Cybersecurity Industry Development and Ecosystem Enablement
EG-CERT will contribute to fostering a robust national cybersecurity ecosystem by:

- Supporting the development and licensing of cybersecurity service providers.
- Encouraging innovation, startups, and local technology development.
- Strengthening public-private partnerships across telecom, finance, and digital platforms.

CONCLUSION

2025 marked a year of consolidated operational excellence, ecosystem maturation, and strengthened international positioning for EG-CERT and Egypt's broader cybersecurity community. Egypt's first-place finish in the ITU Global CyberDrill 2025, its signature of the UN Cybercrime Convention in Hanoi, the deepening of the NTRA cybersecurity services regulatory regime, and continued investment in youth talent development collectively reflect the ongoing execution of Egypt's National Cybersecurity Strategy 2023–2027. EG-CERT's visible role continued to expand beyond incident response into a broader enabling function – supporting Egypt's cybersecurity market, innovation pipeline, and international standing.

EGYPT

EG-FINCIRT

مركز الاستجابة لطوارئ الحاسب الآلي للقطاع المصرفي
EG FINCIRT

Summary of Major Activities

In 2025, the EG-FinCIRT team successfully enhanced its detection and response capabilities through the expansion and strengthening of its infrastructure across financial constituents.

In parallel, it broadened its collaboration landscape with both national and international partners, while further advancing its threat intelligence operations and information-sharing capabilities.

This expanded infrastructure provides a comprehensive view of traffic across the Egyptian financial sector, supporting proactive threat hunting, effective coordination of major incident response, and enhanced threat intelligence collaboration and exchange.

Achievements

EG-FinCIRT alerted constituents with 279 vulnerabilities, including 106 classified as critical, and provided guidance on appropriate mitigation actions to help ensure their security as early as possible. Additionally, EG-FinCIRT successfully responded to 65 incidents that required the engagement of the DFIR team to detect the root cause, ensure proper scoping, effective mitigation, and thorough remediation efforts.

Moreover, EG-FinCIRT implemented enhancements to the Malware Analysis Lab, which significantly improved the capability to detect and analyze newly discovered samples. enabling us to promptly alert constituents with identified indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs).

Furthermore, EG-FinCIRT improved the threat-sharing platform to support more effective monitoring, collaboration, response, and sharing.

Finally, EG-FinCIRT R&D team is also working on developing an Anti-DDoS attack solution for financial sector.

ABOUT ORGANIZATION

Egyptian Financial Computing Incident Response Team - EG-FinCIRT Established in 2018, EG-FinCIRT serves as the cornerstone of Egypt's national cybersecurity infrastructure, specifically designed to assist in protecting the financial sector from evolving digital threats. As the sector's

central cybersecurity hub, EG-FinCIRT provides specialized incident response and expert guidance to help constituents identify, prevent, detect, and recover from cyber-attacks.

EG-FinCIRT Mandate:
EG-FinCIRT is dedicated to supporting the mitigation of cyber-attack impacts, maintaining forensic integrity during investigations, and strengthening the overall cybersecurity maturity of the sector. Acting as a central hub for threat intelligence and providing guidance on critical security incidents, we contribute to safeguarding the integrity of the financial system, thereby enhancing economic confidence and promoting foreign investment in Egypt.

ACTIVITIES & OPERATION

Scope and definitions

The scope of EG-FinCIRT activities extends across the entire financial sector, encompassing banks and financial institutions. These efforts include proactive threat monitoring, incident detection and response, digital forensics and malware analysis, and threat intelligence sharing.

The aim is to build a resilient cybersecurity environment that safeguards critical financial infrastructure, ensures compliance with regulatory standards, and minimizes the impact of cyber threats.

Additionally, the scope includes raising cybersecurity awareness, and guiding institutions in implementing best practices and robust security controls to strengthen their overall cyber posture.

Incident handling reports

Throughout 2025, EG-FinCIRT managed a total of 65 cybersecurity incidents, of which 7 were classified as critical, 30 identified as high severity, and 28 assessed as medium-level threats.

These incidents were detected using EG-FinCIRT Infrastructure and it varies between malware infections, Distributed Denial of Service (DDoS) attacks, and exploitation of vulnerabilities.

Abuse statistics

The abusive statistics will include detected/reported phishing campaigns along with detected domains attempting to masquerade as legitimate ones to deceive victims.

EG-FinCIRT monitors these domains as soon as they are created to ensure they are not involved in malicious activities. If EG-FinCIRT detects any masquerading or malicious behavior, EG-FinCIRT takes the necessary steps to take down the domain.

The statistics will also cover the proper configuration of SPF and DMARC for domains and subdomains, ensuring that our constituents are protected from domain spoofing. For the statistics, the phishing campaigns were 317, and 149 domains take downs.

Publication(s)

EG-FinCIRT published cybersecurity alerts on EG-FinCIRT website. Below is the categorization of the published alerts

Critical Alerts Published	106
High Alerts Published	167
Medium Alerts Published	6
Total Number	**279**

New service(s)

Establishing a Research and Development Team: The R&D team is focused on developing innovative solutions to enhance cybersecurity resilience and deliver a comprehensive defense posture across the Egyptian financial sector.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- Strategic Visit by the Bank of Kenya: EG-FinCIRT hosted a delegation from the Bank of Kenya, facilitating the exchange of best practices and sharing insights from its pioneering role in banking cybersecurity.
- Technical Delegation Visit from the Bank of Tanzania: EG-FinCIRT hosted a delegation from the Bank of Tanzania to showcase its pioneering cybersecurity experience in the financial and banking sectors.

Events involvement

- 37th Annual FIRST Conference - (June 22 - 27, 2025, In Copenhagen, Denmark)
- Arab Security Conference 2025 - (September 7 – 8, 2025, Cairo, Egypt)
- Cyber Threat Intelligence Conference 2025 – (April 21-23, 2025, In Berlin, Germany)
- Black Hat Asia 2025 and AI Summit - (April 2 - 4, 2025, Singapore)
- Black Hat USA 2025, AI Summit and DefCon - (August 5 - 10, 2025, Las Vegas)
- GITEX Africa Morocco 2025 - (April 14 – 16, 2025, in Marrakech, Morocco)
- RSA Conference 2025 - (April 28 – May 1, 2025, in San Francisco, USA)
- GISEC Global 2025 - (May 6 – 8, 2025, in Dubai, UAE)
- CaiSec 2025 - (May 25 – 26, 2025, Cairo, Egypt)
- IT Security Summit - (June 16 – 19, 2025, in Berlin, Germany)
- 17th annual OIC-CERT conference and the 13th Arabic Regional, OIC-CERT & Africa Cyber Drill. (September 15 – 19, 2025, in Rabat, Morocco)

- Singapore International Cyber Week 2025 - (October 20 – 25, 2025, Singapore)
- Global Cyber Conference 2025 - (October 22 – 23, 2025, in Zurich, Switzerland).
- Kaspersky Security Analyst Summit 2025 - (October 26 – 29, 2025, in Khao Lak, Thailand)

Achievements

Key Enhancements and Upgrades

- Implemented advanced technological upgrades to platforms and devices supporting continuous monitoring services.
- Strengthened threat intelligence and alert management capabilities.
- Improved detection accuracy and response efficiency.
- Enhanced overall situational awareness across the financial sector.
- Increased visibility and improved data processing capabilities.
- Integrated advanced security controls across systems.

2026 PLANNED ACTIVITIES

Establishing a Cyber Incident Response Capabilities Measurement Platform (Cyber Drill) – Under Study / Request for Information Phase:

This project aims to move beyond traditional tabletop exercises by establishing a comprehensive "Cyber Battle" ecosystem. It will create a realistic, on-premises environment to test, measure, and strengthen cyber defense readiness across the Egyptian financial sector, supporting key strategic objectives within the banking industry.

The platform will enable realistic cyber-attack simulations by replicating the national banking digital environment, allowing advanced Red Team vs. Blue Team exercises to assess and analyze incident response capabilities.

It will also support industry-specific scenario testing, tailored to the banking sector, including simulations of core banking services and inter-bank transactions.

In addition, the platform will provide performance measurement and scoring through quantitative readiness metrics, including live scoring and gap analysis.

Finally, it will support compliance by helping banks validate their security controls against critical regulatory and cybersecurity standards.

Developing/building Anti-DDoS Solution:

EG-FinCIRT R&D team is also working on developing an Anti-DDoS solution for financial sector.

CONCLUSION

Collectively, these infrastructure expansions and technological advancements represent a significant milestone in EG-FinCIRT's continuous evolution toward a more scalable, intelligence-driven, and resilient cybersecurity ecosystem. By enhancing connectivity with a wider network of banks and financial institutions, modernizing continuous monitoring capabilities, and operationalizing centralized threat intelligence orchestration, EG-FinCIRT has substantially strengthened sector-wide cyber defense readiness. These initiatives not only improve detection precision and response agility but also reinforce coordinated protection, operational continuity, and long-term cyber resilience across the Egyptian financial sector.

Beyond technical implementation, 2025 solidified our position as a global and regional leader in financial cybersecurity. Our active engagement in premier international forums—including the 37th Annual FIRST Conference in Denmark, Singapore International Cyber Week, and the 17th annual OIC-CERT conference in Morocco—facilitated vital knowledge exchange and fostered technical partnerships with global authorities. These engagements, alongside strategic technical visits from delegations such as the Bank of Kenya and Bank of Tanzania, represent a long-term investment in our human capital.

As we look toward the future, the ongoing development of the Cyber Incident Response Capabilities Measurement Platform (Cyber Drill) remains a central pillar of our mission. By moving from theoretical readiness to a battle-tested posture, EG-FinCIRT continues to provide a "bank-grade" defense that reinforces economic stability and secures the integrity of Egypt's financial system.


2025
Arab Security Conference
9th Round
Dr. Sherif Hazem
Sub-Governor Cyber Security
of Central Bank Of Egypt
OPENING KEYNOTES
SPEAKER 2025


FDC
SUMMIT
FDC SUMMIT OPENING CEREMONY
DR. Sherif Hazem
Sub-Governor Cyber Security
Central Bank of Egypt

INDONESIA

ID-SIRTII/CC

DEPUTI BIDANG OPERASI KEAMANAN SIBER DAN SANDI
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

HIGHLIGHTS OF 2025

Summary of Major Activities

In 2025, a total of 5,515,394,886 anomalous traffic activities were detected in Indonesia. The most dominant anomaly was Mirai Botnet, accounting for 2,124,835,234 activities. Mirai Botnet is a type of botnet that primarily targets Internet of Things (IoT) devices and is commonly used to launch Distributed Denial of Service (DDoS) attacks against websites or online services, potentially causing service disruptions or downtime. During the same period, there were 39,685,439 Advanced Persistent Threat (APT) activities, 13,915,440 ransomware activities, and 246,288,299 phishing activities recorded. Id-SIRTII/CC issued 2,821 incident indication notifications to stakeholders, with data breach incidents representing the most frequently reported notification type.

Based on Cyber Threat Intelligence monitoring and analysis, Id-SIRTII/CC also identified 254 indications of data breach incidents. Investigations conducted on the darknet revealed 44,772,291 exposed data findings affecting 461 stakeholders in Indonesia. In addition, 4,433 web defacement incidents were detected targeting various domains, including 1,915 cases related to online gambling attacks against government websites. Through the cyber complaint service, Id-SIRTII/CC received 1,965 reports from stakeholders and published 144 cybersecurity advisories throughout the year. One of the national Top CVEs with a critical Common Vulnerability Scoring System (CVSS) rating was CVE-2020-0796 in Microsoft Windows SMBv3, which allows threat actors to execute commands with system privileges, install malware, modify or delete data, and create new administrative accounts. Furthermore, Id-SIRTII/CC conducted IT Security Assessment (ITSA) activities and identified 1,689 vulnerabilities across 368 tested applications, consisting of 134 critical, 455 high, 656 medium, 223 low, and 221 informational vulnerabilities affecting web, mobile, and infrastructure systems.

Furthermore, Id-SIRTII/CC, acting on behalf of Indonesia as Deputy Chair of the OIC-CERT Board and lead for the 3rd Pillar on Cybersecurity Talent Development, has successfully fulfilled its strategic mandate to establish specialized cybersecurity training programs and cybersecurity capacity building awareness programs for OIC-CERT members. From July to October 2025, Id-SIRTII/CC designed and delivered four high impact capacity building webinars, thereby achieving 100% completion of both KPIs by October 2025 and reinforcing Indonesia's leadership and commitment within the OIC-CERT community.

The 2025 online seminar series was thematically structured to address advanced and emerging cybersecurity challenges across technical, operational, and strategic domains. The first online seminar on "Uncovering Data Breaches: A Forensic Approach to Tracing the Attack" showcased Indonesia's innovation through the KARAFFE forensic framework and ARKAIV machine learning–based exfiltration prediction. The second online seminar, "Offensive Mobile Security: Advanced Penetration Testing for Mobile Applications", deepened practitioners' skills in mobile and API penetration testing aligned with OWASP standards. The third online seminar, "Securing Digital Identities: The Role of Identity Brokers in Modern Cybersecurity", brought together Indonesian and Bruneian experts to discuss digital identity frameworks, Zero Trust, and future trends such as SSI and post-quantum cryptography. The fourth online seminar, "OSINT/Dark Web Investigation: Cyber Threat Intelligence: Using OSINT & Dark Web Data for Security Operations", highlighted the integration of OSINT and Dark Web monitoring into national CTI operations. In total, the four webinars engaged 876 participants (392, 89, 272, and 123 respectively) from BSSN, OIC-CERT, and Id-SIRTII/CC constituents, underscoring strong regional interest and positioning the program as a flagship initiative under the 3rd Pillar.

Notwithstanding these substantial achievements, several strategic challenges remain. First, participation from OIC-CERT members, while present, has not yet reached its optimal potential; out of the total participants, direct representation from OIC-CERT member organizations is still relatively limited compared to national constituents, indicating the need for more aggressive outreach, targeted engagement, and co-branding with member countries. Second, the level of knowledge uptake and practical application of the materials delivered has not yet been systematically measured; standardized evaluation mechanisms such as pre- and post-assessments, longitudinal feedback, and impact tracking have yet to be fully implemented. Addressing these challenges in future cycles will be crucial to deepening member-country engagement, demonstrating measurable capacity gains, and further elevating the strategic value of OIC-CERT's Cybersecurity Talent Development pillar.

Achievements

During 2025, Indonesia, represented by Id-SIRTII/CC, actively participated in several regional and international cybersecurity competitions and innovation initiatives. These activities aimed to strengthen technical capabilities, foster innovation, and enhance collaboration with cybersecurity communities across the ASEAN region and beyond. Through participation in various Capture the Flag (CTF) competitions, hackathons, and capacity-building programs, the delegation demonstrated strong technical competence and achieved several notable accomplishments that contributed to the reputation of Indonesia in the regional cybersecurity ecosystem.

Cyber Battle: Capture The Flag (CTF) 2025 – Brunei Darussalam

The Indonesia contingent represented by Team Id-SIRTII/CC achieved 1st place among 16 teams in the Cyber Battle CTF 2025, held alongside the Cyber Security Conference (CySec) 2025 on 15–16 September 2025 in Brunei Darussalam, organized by ITPSS Sdn Bhd in collaboration with Cyber Security Brunei (CSB) and the Brunei Cybersecurity Association (BCSA).

BeAI Hackathon 2025
Team Leaklens from the Directorate of Cyber Security Operations secured 2nd place in the BeAI Hackathon with an AI-based threat intelligence lifecycle tool designed to detect compromised servers, exposed credentials, and sensitive data leaks, demonstrating innovation in applying artificial intelligence to enhance cybersecurity operations.

Cyber SEA Games 2025 – Thailand
The Indonesia contingent represented by Team Id-SIRTII/CC achieved 3rd place at the Cyber SEA Games 2025 organized by AJCCBC in Bangkok, Thailand (16–17 October 2025). Additionally, three Indonesian team members were selected to represent ASEAN at the International Cybersecurity Challenge (ICC) 2025.

3rd ASEAN Cyber Shield (ACS) Hacking Contest 2025
Team Id-SIRTII/CC secured 2nd place in the regional competition organized by AKCF and KISA, which featured CTF Jeopardy and Attack–Defense scenarios covering multiple cybersecurity domains including reverse engineering, cryptography, forensics, OSINT, and web exploitation.

ABOUT ORGANIZATION

The government agency, which has a national responsibility in cybersecurity, started with the establishment of Id-SIRTII/CC on 4th May 2007 by the Minister of Communication and Information Decree number 26 in 2007. Since the establishment until 2018, Id-SIRTII/CC assumed the function as the National CSIRT and Coordination Centre for national incident handling and works under the Directorate of Telecommunication of the Ministry of Communication and Information. Based on the Presidential Decree Number 53 in 2017, Id-SIRTII/CC merged and moved to Badan Siber dan Sandi Negara (NCCA).

In April 2018, NCCA officially started carrying the strategic roles as the top-level authority for cybersecurity related activities in Indonesia. The agency is directly under the purview of the President, which is the merging of Id-SIRTII/CC and the National Crypto Agency (Lembaga Sandi Negara - LSN). Id-SIRTII/CC is currently operating under the Directorate of Cyber Security Operation, Deputy of Cyber and Crypto Security Operations, NCCA.

ACTIVITIES & OPERATION

Scope and definitions

Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) plays a crucial role in cybersecurity for Indonesia's internet infrastructure. Its scope includes threat monitoring, incident handling, and regulatory compliance. By coordinating prevention, detection, and response measures, Id-SIRTII/CC helps mitigate cybersecurity risks across various sectors. It also works alongside law enforcement agencies to ensure adherence to cybersecurity laws and supports public awareness initiatives through education and training. The annual reports published by Id-SIRTII/CC provide insights into key activities and developments within Indonesia's cybersecurity landscape. These reports typically cover incident trends, threat

analysis, regulatory updates, and strategic initiatives undertaken throughout the year. They serve as a valuable resource for stakeholders seeking to understand the evolving cybersecurity challenges and the measures being implemented to address them. Additionally, Id-SIRTII/CC contributes to security infrastructure development by maintaining databases, analysis tools, and monitoring systems that enhance the country's digital resilience. By fostering collaboration among government institutions, private organizations, and academic researchers, Id-SIRTII/CC aims to strengthen Indonesia's cybersecurity posture while adapting to emerging threats.

Incident handling reports

NCCA has carried out 35 cyber incident response assistance activities involving 34 stakeholders. The implementation falls into the following three categories:

Handled by Id-SIRTII/CC
There were 12 incidents in which the cyber incident handling assistance process was carried out entirely by Id-SIRTII/CC.

Collaboration handling by Id-SIRTII/CC and Organizational CSIRT
There were 10 incidents in which the cyber incident handling assistance process was carried out entirely by Id-SIRTII and Organizational CSIRT.

Handled by Organizational CSIRT
There were 13 incidents in which the cyber incident handling assistance process was carried out entirely by Organizational CSIRT.

The following is the classification of incidents handled by the Cyber Incident Response Assistance Service:

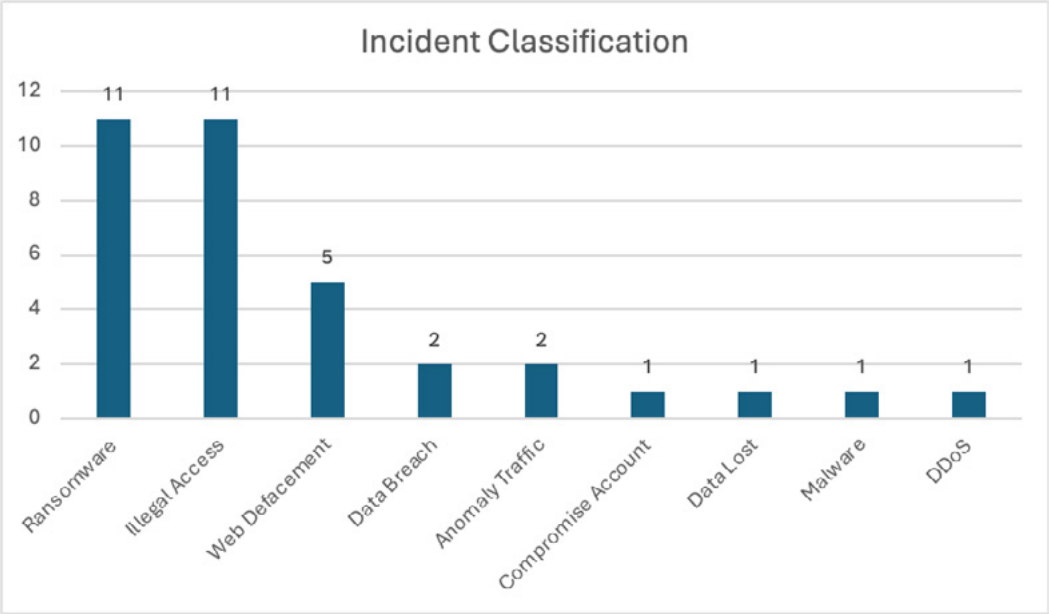


Figure 1. classification of incidents handled by Id-SIRTII/CC.

Among the 35 incidents assisted, the most frequent cases in 2025 were Ransomware, Illegal Access, Web Defacement, and other types of incidents.

The following are the lessons learned from one of the major incidents that occurred in Indonesia, namely the ransomware incident. A ransomware incident is a cyberattack caused by malware that infects a device and encrypts the data stored on it. Once the device is infected, the ransomware encrypts critical files, rendering them inaccessible. The threat actor then demands a ransom, usually in the form of digital currency, in exchange for restoring access to the encrypted data.

Ransomware attacks not only cause financial losses but can also disrupt business operations and damage an organization's reputation. To prevent ransomware attacks, it is crucial to regularly back up data, use reliable antivirus software, and consistently update operating systems and applications. To prevent ransomware incidents, CSIRT can implement the following lessons learned:

Strengthening Initial Access and Credential Security
Ransomware highlights the importance of securing the system's initial access points. All applications and services connected to the internet must be regularly updated, securely configured, and supported by strong password policies as well as the use of multi-factor authentication (MFA) to prevent the misuse of legitimate accounts.

Monitoring Command Execution and Endpoint Activity
The use of command-line tools, scripts, and malware on endpoints indicates the need for strong endpoint protection. The implementation of antivirus, EDR, firewalls, and system activity logging is essential to detect and respond to suspicious activities before ransomware spreads more widely.

Limiting Lateral Movement through Network Segmentation
The spread of ransomware to other systems can be prevented through effective network segmentation. The implementation of VLANs, inter-segment firewalls, micro-segmentation, and the Zero Trust principle helps limit communication between systems and reduce the impact of an attack.

Strictly Managing Accounts and Access Privileges
The use of accounts with high privileges can increase the impact of an incident. Therefore, organizations need to implement the principle of least privilege, conduct periodic access reviews, and restrict the use of administrator accounts only to specific needs.

Ensuring Data Backups are Secure and Isolated
Data backups are a key element in ransomware recovery. The backup process should be performed regularly, using appropriate methods (full, incremental, or differential), stored in a separate location, and periodically tested to ensure that data can be restored without relying on ransom payments.

Enhancing Response Readiness and Management Support
Incident detection and response readiness must be supported by clear procedures, regular simulation exercises, and cross-team coordination. Support from top management is essential in providing resources, making strategic decisions, and ensuring that security policies remain relevant and effective.

Abuse statistics

Anomaly Traffic Trend

In 2025, the total volume of anomalous traffic detected in Indonesia reached 5,462,352,220 incidents. The highest level of anomalous traffic occurred in May, with 755,639,091 incidents, while the lowest level was recorded in December, with 213,041,476 incidents. The significant increase observed in May is associated with the global surge in Mirai Botnet activities during that period.

No	Month	Amount
1	January	425,942,679
2	February	401,591,752
3	March	371,189,964
4	April	548,480,531
5	May	755,639,091
6	June	573,606,757
7	July	567,717,476
8	August	420,813,410
9	September	386,728,019
10	October	431,045,086
11	November	366,555,979
12	December	266,084,143

Such anomalous traffic activities may lead to several adverse impacts, including degradation of device and network performance, theft of sensitive data, reputational damage, and a decline in organizational trust. Figure below illustrates the monthly distribution of anomalous traffic recorded throughout 2025.

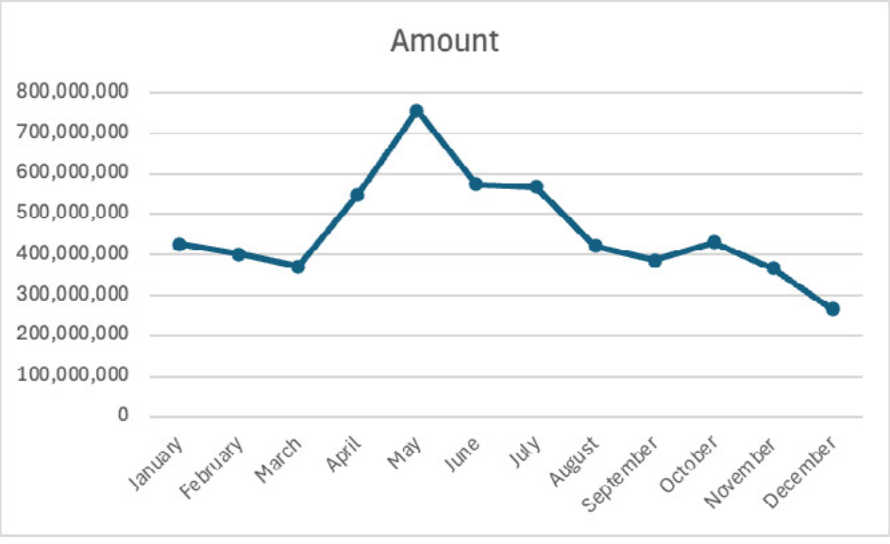


Figure 2. The number of traffic anomalies in Indonesia in a year.

Top 10 Anomaly Traffic

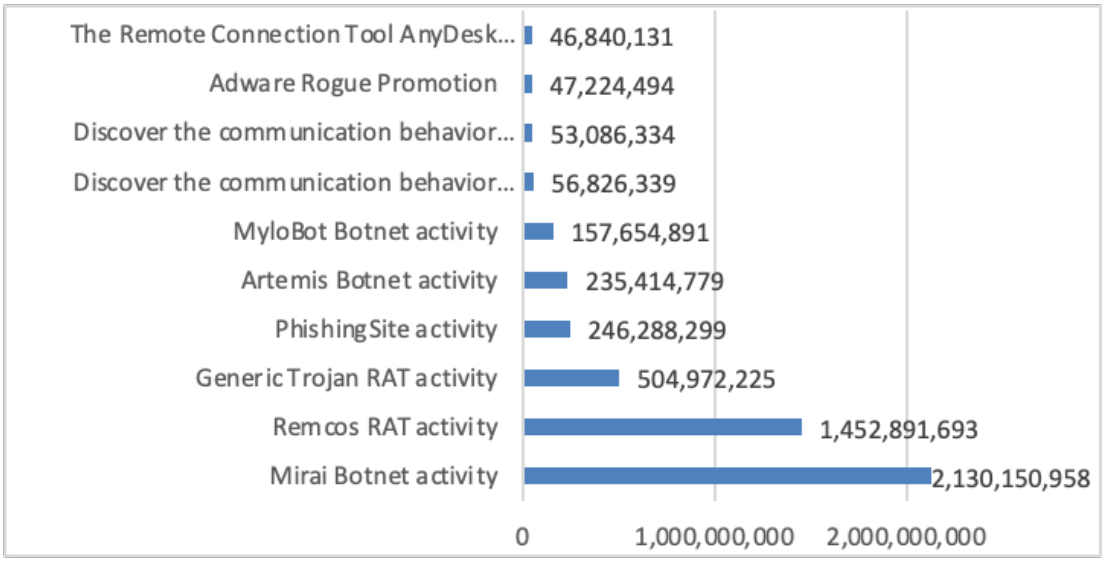


Figure 3. Top 10 traffic anomalies.

No	Anomaly Traffic	Summary
1	Mirai Botnet	2,130,150,958
2	Remcos RAT	1,452,891,693
3	Generic Trojan RAT	504,972,225
4	PhishingSite	246,288,299
5	Artemis Botnet	235,414,779
6	MyloBot Botnet	157,654,891
7	Discover the communication behavior of VPN tool OpenVPN	56,826,339
8	Discover the communication behavior of the VPN tool WireGuard	53,086,334
9	Adware Rogue Promotion	47,224,494
10	The remote connection tool AnyDesk is active	46,840,131

Cybersecurity monitoring throughout 2025 identified several dominant threats targeting networks and information systems, particularly those associated with botnet and malware activities. Among the most notable threats were Mirai Botnet, Artemis Botnet, and MyloBot Botnet, which primarily infect vulnerable devices and enable threat actors to remotely control compromised systems. These botnets are often used to conduct Distributed Denial of Service (DDoS) attacks, distribute spam, steal sensitive data, and deploy additional malicious payloads. Such infections may significantly degrade device and network performance, increase the risk of data breaches, and potentially involve compromised devices in large-scale malicious activities without the owners' knowledge. Preventive measures include strengthening device security configurations, updating operating systems and firmware, using up-to-date antivirus protection, and continuously monitoring network traffic.

In addition, various trojan and credential-stealing threats were observed, including Remcos RAT, Generic Trojan RAT, and phishing-related malware activities. These threats commonly spread through phishing emails, malicious attachments, or fraudulent websites designed to deceive users into disclosing sensitive information. Once a system is compromised, attackers may gain unauthorized access to devices, steal confidential information, capture screenshots, perform keylogging, or manipulate files and system configurations. These activities may lead to identity theft, financial losses, and unauthorized access to critical organizational systems. To mitigate these risks, organizations and users are encouraged to implement secure email practices, restrict user privileges, install software only from trusted sources, and maintain regular system and application updates.

Furthermore, several network-related anomalies and potentially risky tools were also detected, including activities associated with VPN applications such as OpenVPN and WireGuard, the remote access tool AnyDesk, and Adware Rogue Promotion. While some of these tools may have legitimate uses, they may also be exploited by threat actors to conceal malicious communications, conduct espionage activities, or gain unauthorized remote access to systems. In addition, adware-related activities may expose systems to malicious redirects, unwanted software installations, and further security vulnerabilities. To reduce these risks, organizations should implement strong firewall configurations, enforce strict access control policies, conduct regular security audits, monitor network traffic and logs, and apply secure configuration and segmentation practices across their infrastructure.

Advanced Persistent Threat Activity

During the reporting period, a total of 139.685.439 Advanced Persistent Threat (APT) activities were detected. APT refers to an attack campaign conducted by cyber threat actors, whether state-sponsored or non-state-sponsored. These actors employ sophisticated methods and techniques designed to carry out persistent, stealthy cyberattacks. Such operations aim to gain unauthorized access to target systems and maintain a long-term presence without detection by security mechanisms. The primary objective of these threat groups is to access, monitor, and exfiltrate valuable information from targeted systems or networks. This includes corporate confidential data, financial records, or high-tech intellectual property, with the intent of enabling long-term strategic exploitation.

One notable APT case identified in Indonesia involves the OceanLotus group. This group was revealed to target government institutions, private organizations, and strategic sectors across Southeast Asia. Based on anomalous traffic monitoring results, the following chart presents the top 5 most frequently detected APT groups within Indonesian cyberspace:

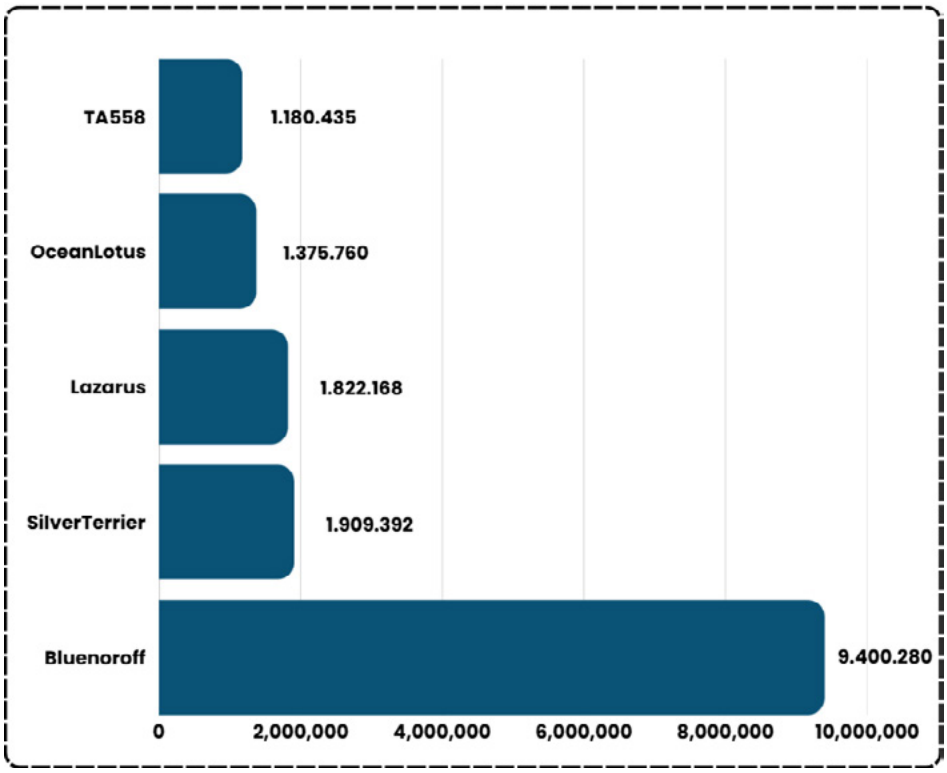


Figure 4. Top 5 most frequently detected APT groups.

Based on Figure 4, five Advanced Persistent Threat (APT) groups were most frequently detected targeting Indonesian cyberspace. The findings from anomalous traffic monitoring conducted throughout 2025 reveal significant variations in threat actor activity levels. Bluenoroff emerged as the most prevalent threat, with 9,400,280 detected incidents, surpassing all other identified APT groups. This figure represents approximately 65% of the total APT-related malicious traffic observed, indicating a concentrated and persistent campaign against Indonesian digital infrastructure. The disproportionate volume of Bluenoroff activity warrants particular attention, as it suggests either an intensified focus on Indonesian targets or the deployment of more aggressive operational tactics compared to other threat actors.

The remaining four APT groups demonstrated comparable activity levels:

- SilverTerrier: 1,909,392 incidents
- Lazarus: 1,822,168 incidents
- OceanLotus: 1,375,760 incidents
- TA558: 1,180,435 incidents

The disproportionate volume of Bluenoroff activity warrants particular attention, as it suggests either an intensified focus on Indonesian targets or the deployment of more aggressive operational tactics compared to other threat actors.

Ransomware Activity

During the reporting period, a total of 13,915,440 ransomware activities were detected. Ransomware represents a critical threat vector, utilizing malicious encryption techniques to lock victim data, including documents, systems, and devices, rendering them inaccessible. Following the encryption, perpetrators demand ransom payments in exchange for data recovery. These

attacks target a wide spectrum of victims, ranging from individuals and private companies to government institutions, with impacts including data loss, financial damage, reputational harm, and disruption of public services.

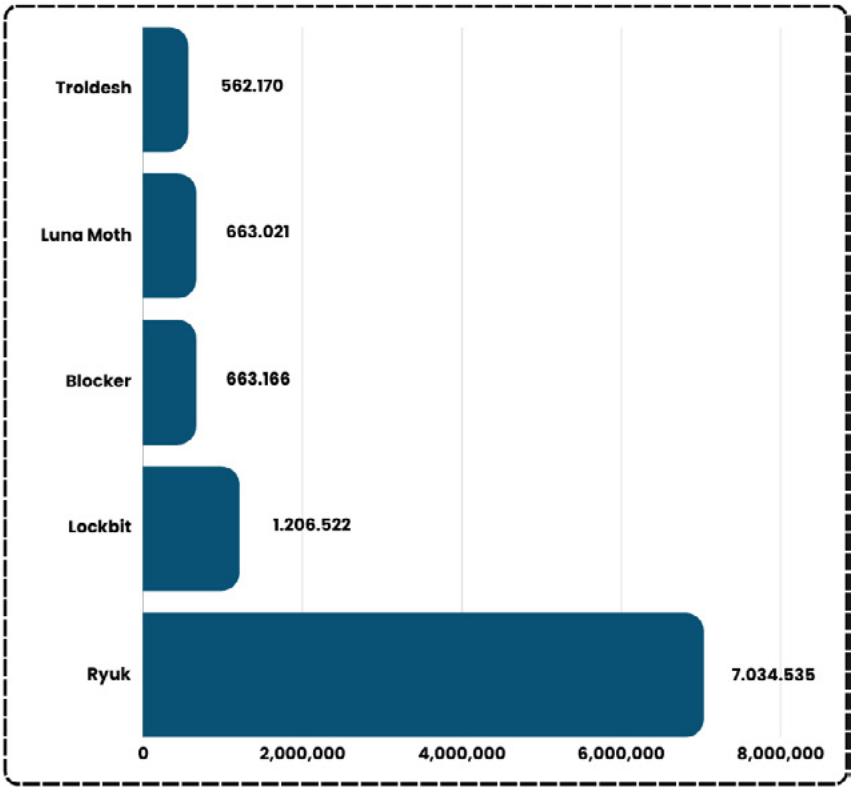


Figure 5. Top 5 most frequently detected Ransomware.

Based on Figure 5, Analysis of the top five most prevalent ransomware families reveals a clear dominance of Ryuk, which accounted for 7,034,535 detected incidents. This represents approximately 50.5% of all ransomware activity observed, indicating that Ryuk remains the primary ransomware threat to Indonesian digital infrastructure. The remaining ransomware families showed significantly lower but still concerning activity levels:

- LockBit: 1,206,522 incidents
- Blocker: 663,166 incidents
- Luna Moth: 663,021 incidents
- Trolldesh: 562,170 incidents

The substantial gap between Ryuk and other ransomware variants suggests either a highly targeted campaign or particularly effective distribution mechanisms employed by this threat group.

Phishing

Phishing remains one of the most prevalent cyberattack forms, utilizing social engineering techniques to impersonate trusted entities. These attacks typically occur via email, text messages, or fake websites containing malicious links or attachments. The primary objective is to deceive victims into interacting with these elements, thereby enabling malware execution on their devices. Throughout 2025, a total of 246,288,299 phishing activities were identified within

Indonesian cyberspace. Phishing attacks pose a significant risk as they often serve as the initial entry point for malware installation or unauthorized system access. The monthly distribution of these activities reveals distinct fluctuations over the reporting period in Figure 6.

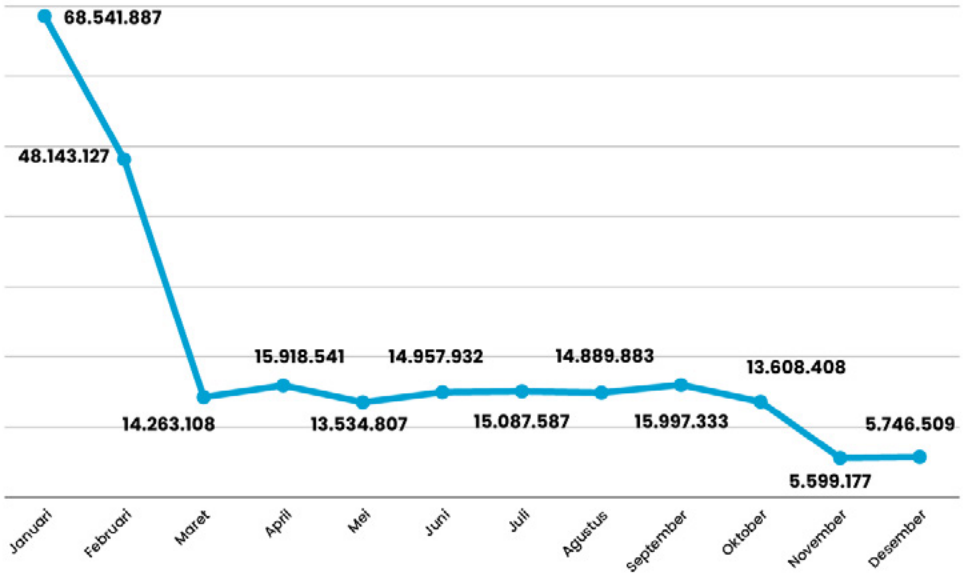


Figure 6. Monthly Report Phishing Distribution.

January recorded the highest volume of phishing attempts, reaching 68,541,887 activities. February followed with the second highest volume at 48,143,127 activities. This concentrated activity at the beginning of the year accounts for a massive portion of the total annual threats. Following February, activity levels dropped sharply in March to 14,263,108 and remained stable through October, fluctuating between approximately 13 million and 16 million incidents per month. The lowest activity level was observed in November, with only 5,599,177 recorded incidents. Activity slightly recovered in December to 5,746,509.

Publication(s)

Id-SIRTII/CC has published several cybersecurity-related documents that can be leveraged by stakeholders in Indonesia. These documents include cybersecurity news publications (Cyber Blitz), monthly reports, annual reports, and security advisories.

Cyber Blitz is a document published by Id-SIRTII/CC that contains news and information related to international cybersecurity developments. The content is current and based on reliable references. Examples of the information included in this document cover cyber-attacks conducted by threat actors, cyber incidents affecting international organizations, updates on technological developments, vulnerabilities and security weaknesses in applications or systems, as well as other cybersecurity-related information. Through this document, it is expected that stakeholders in Indonesia will obtain up-to-date information on global cybersecurity developments.

Id-SIRTII/CC also regularly produces monthly reports related to cybersecurity developments in Indonesia. These reports provide an overview of cyber-attacks detected targeting Indonesia, regional and international activities attended by Id-SIRTII/CC personnel in strengthening Indonesia's cybersecurity capacity, as well as a recap of services provided by Id-SIRTII/CC to

its stakeholders. These monthly reports are subsequently consolidated into an Annual Report, which presents an overview of cybersecurity developments in Indonesia throughout the year.

Security advisories are official notifications intended to inform stakeholders about newly discovered vulnerabilities, emerging security threats, or other cyber risks. These advisories typically provide a description of the vulnerability or threat, the affected systems or products, the potential impact, and recommended mitigation measures such as patches, configuration changes, or security best practices. The purpose of these advisories is to provide timely and reliable information so that organizations and users can take appropriate actions to protect their systems and reduce the risk of cyber incidents.

The number of each of these documents is as follows:
- Cyber Blitz 236 publications;
- Monthly reports 12 publications;
- Annual report 1 publication;
- Security Advisories 143 publications.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

Webinar Workshop 1: Offensive Mobile Security: Advanced Penetration Testing for Mobile Applications

The online seminar titled "Offensive Mobile Security: Advanced Penetration Testing for Mobile Applications" featuring Ardya Suryadinata, S.S.T.TP., M.Eng was held on 26 August 2025 and attended by 89 participants from NCCA, OIC-CERT, and Id-SIRTII constituents. The session highlighted the growing importance of mobile application penetration testing due to the increasing use of mobile devices and the sensitive data stored on them. The speaker explained key testing approaches based on the OWASP Mobile Top 10 and OWASP API Security Top 10, including environment preservation testing, API testing, static and dynamic analysis, and reverse engineering. From a defensive perspective, the session emphasized the implementation of OWASP MASVS/MASTG standards, secure storage practices, TLS pinning, and strong server-side validation and authorization. The discussion also noted that penetration testing can be performed using both real devices and emulators with minimal differences, while applications built with Flutter are more complex and require more time to test.

Webinar Workshop 2: OSINT/Dark Web Investigation: Cyber Threat Intelligence: Using OSINT & Dark Web Data for Security Operations

The capacity building online seminar titled "OSINT/Dark Web Investigation: Cyber Threat Intelligence – Using OSINT and Dark Web Data for Security Operations" was held on 30 October 2025 and attended by 123 participants from BSSN, OIC-CERT, and Id-SIRTII constituents. The session highlighted the importance of utilizing Open-Source Intelligence (OSINT) and Dark Web data to strengthen Cyber Threat Intelligence operations in response to the increasing volume of cyber activities across open and hidden online environments. The presenter explained how OSINT can be used to collect and analyse publicly available information from sources such as social media, forums, domains, and code repositories to detect potential cyber threats and

data leaks. The online seminar also introduced investigative methodologies and tools including Maltego, SpiderFoot, Recon-ng, Tor Browser, Ahmia, and DarkSearch for conducting link analysis, metadata analysis, and Dark Web correlation. The discussion emphasized the need to integrate OSINT, Dark Web monitoring, and organizational data into a national CTI framework to support proactive threat hunting, incident response, and adaptive cybersecurity operations.

Awareness Program 1: Uncovering Data Breaches: A Forensic Approach to Tracing the Attack

The capacity building online seminar titled "Uncovering Data Breaches: A Forensic Approach to Tracing the Attack" was held on 29 July 2025 and attended by 392 participants from BSSN, OIC-CERT, and Id-SIRTII constituents. The session introduced a digital forensic approach for investigating data breach incidents using the KARAFFE forensic framework and ARKAIV machine learning model for predicting data exfiltration. KARAFFE focuses on evidence examination and analysis through Data Breach Breakdown mapping and the 5WH approach (What, Who, When, Where, Why, and How) to support structured investigations of compromised systems. ARKAIV is designed to automatically predict the likelihood of data exfiltration using machine learning techniques such as SMOTE and SMOTE+ENN, achieving high accuracy by utilizing threat reports, event logs, and the MITRE ATT&CK framework. The presenter also explained that both tools are based on international standards such as NIST SP 800-88 and ISO/IEC 27043 and are currently under further development to support artificial intelligence capabilities and cloud-native environments.

Awareness Program 2: Securing Digital Identities: The Role of Identity Brokers in Modern Cybersecurity

The capacity building online seminar titled "Securing Digital Identities: The Role of Identity Brokers in Modern Cybersecurity" was held on 24 September 2025 and attended by 272 participants from NCCA, OIC-CERT, and Id-SIRTII constituents. The session featured two speakers, Faizan Aditya from BLPID Indonesia and Muhammad Hanif Jumat from Cyber Security Brunei, who discussed the growing importance of digital identity in modern cybersecurity. The first presentation introduced the Digital Trust Framework and Digital Identity Wallet concept, emphasizing secure credential management and the development of integrated digital public infrastructure supported by international standards and national regulations. The second presentation highlighted the implementation of digital identity systems in Brunei and the role of Zero Trust Architecture in ensuring secure access through strong authentication, device validation, and continuous monitoring. The discussion also addressed key challenges and future trends, including regulatory alignment, scalability, and the shift toward decentralized and self-sovereign identity models supported by blockchain technology and post-quantum cryptography.

Events involvement

UNODC-IASC Digital Forensic and Evidence Training

The United Nations Office on Drugs and Crime (UNODC), in collaboration with the International Anti-Slavery Commission (IASC), organized a specialized training titled "Digital Forensic and Evidence Training" from 12–14 August 2025, focusing on strengthening cyber investigation capabilities to address cases of human trafficking and exploitation in the digital space. The training was conducted through intensive classroom sessions and simulations using digital forensic tools, where participants were trained to trace digital footprints left by threat actors.

AJCCBC Cybersecurity Technical Training - Network Forensics

The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) organized the 36th Cybersecurity Technical Training on "Advanced Network Forensics" from 19–23 May 2025 in Bangkok, Thailand. The training was attended by 19 cybersecurity professionals from ASEAN member states and aimed to enhance technical capabilities in identifying and responding to complex network threats. The program, opened and closed by the Deputy Secretary-General of Thailand's National Cyber Security Agency, emphasized the importance of regional cooperation and technical expertise in addressing evolving cybersecurity challenges.

International Telecommunication Union (ITU) Global Cyber Drill

The ITU Global Cyber Drill 2025 is an international cyber incident response simulation forum organized by the International Telecommunication Union (ITU) in collaboration with the United Arab Emirates Cyber Security Council. The activity was designed to strengthen the readiness and coordination of stakeholders in responding to various cross-sector and cross-border cyber incident scenarios. The ITU Global Cyber Drill was held from 6–8 May 2025 in Dubai, United Arab Emirates. The event involved participation from various countries, international organizations, and national authorities in the field of cybersecurity, as part of a collective effort to enhance global cyber resilience.

The Conference on Ransomware and Crypto Investigations in Southeast Asia and Cyber Games 2025

The National Cyber Security Agency (NACSA) Malaysia, in collaboration with the Council of Europe and INTERPOL, organized "The Conference on Ransomware and Crypto-Investigations" along with the technical competition Cyber Games 2025, held from 19–23 May 2025 in Kuala Lumpur, Malaysia. The event was attended by more than 120 digital forensic experts and cybercrime investigators from 40 countries, aiming to strengthen international cooperation in addressing ransomware threats and tracking illicit crypto assets. This initiative seeks to build global cyber resilience and establish a new standard for cross-border law enforcement collaboration in the future.

ASEAN Cyber Emergency Response Team Incident Drill (ACID)

The ASEAN Cyber Emergency Response Team Incident Drill 2025 (ACID 2025), held on 21–22 October at the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in Singapore, marked its 20th edition and the first in-person drill since its inception. The activity, organized in conjunction with the Singapore International Cyber Week (SICW), focused on enhancing regional cyber capacity through cross-border exercises in threat intelligence, incident response, and operational cooperation. A total of 36 incident responders participated, representing 11 Member States of the Association of Southeast Asian Nations (ASEAN) and five Dialogue Partners—Australia, India, Japan, South Korea, and China. The Badan Siber dan Sandi Negara (BSSN), as Indonesia's National CSIRT, sent two delegates to participate in the exercise.

AJCCBC Cybersecurity Technical Training Cyber Defense Exercise with Recurrence (CYDER)

The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) training program aims to strengthen the capacity of cybersecurity professionals across ASEAN in responding to increasingly complex cyber threats amid rapid digital transformation. With support from the Japan International Cooperation Agency (JICA), the 38th and 39th AJCCBC Cybersecurity Technical

Trainings were conducted under the theme "Cyber Defense Exercise with Recurrence (CYDER)" focusing on ransomware scenarios and malware analysis. The trainings were held on 17–23 August 2025 and 23–29 November 2025 in Bangkok, Thailand, marking the first implementation of the latest CYDER curriculum.

China–ASEAN Cybersecurity Seminar

The China–ASEAN Cybersecurity Seminar was held from 17–30 June 2025 in Beijing and several other cities in China to strengthen cybersecurity cooperation and capacity building between ASEAN countries and China. Representatives from BSSN participated in lectures, discussions, and field visits covering cybersecurity governance, critical information infrastructure protection, incident response, data protection, artificial intelligence in cybersecurity, and international cooperation practices. The seminar also provided insights into China's integrated cybersecurity ecosystem and the role of CNCERT/CC in national and cross-border incident response, offering valuable references for strengthening Indonesia's cyber diplomacy and regional cooperation.

11th ASEAN Senior Official Meeting on Transnational Crime Working Group on Cyber Crime

The 11th ASEAN Senior Officials Meeting on Transnational Crime Working Group on Cybercrime was held on 24 April 2025 in Singapore and attended by representatives from Singapore, Indonesia, Malaysia, Laos, Thailand, Vietnam, Timor-Leste, and the ASEAN Secretariat. The meeting discussed regional efforts to combat cybercrime, including the growing use of cryptocurrency in illicit transactions related to data breach incidents. Participants also highlighted the increasing threat of information-stealing malware and banking trojans targeting the financial sector, with Vidar, Raccoon Stealer, and RedLine Stealer identified as the most prevalent stealer malware families in the ASEAN region.

UNODC Regional Forum on Enhancing Capabilities Against Cybercrime in Southeast Asia: Focus on Cyber Scams

The United Nations Office on Drugs and Crime (UNODC) organized a regional forum on enhancing capabilities against cybercrime in Southeast Asia, held from 21–23 January 2025 in Manila, Philippines. The event was attended by representatives from Thailand, Malaysia, Indonesia, the Philippines, and Cambodia as part of the UNODC Regional Events on Cybercrime project. The forum aimed to strengthen participants' capabilities in addressing cybercrime, particularly online fraud, through practical discussions on Open-Source Intelligence (OSINT), data analysis, and information verification.

UNODC Regional Meeting on Cyber-Scam Ecosystem and its Implications for Southeast Asia Region

The BSSN team participated in the Regional Meeting on Cyber-Scam Ecosystem and its Implications for Southeast Asia Region, organized by the United Nations Office on Drugs and Crime (UNODC) on 9–10 January 2025 in Vietnam. The meeting was attended by representatives from several Southeast Asian countries, including Indonesia, Thailand, Malaysia, Cambodia, the Philippines, and Singapore. The activity was part of the UNODC project aimed at strengthening the capabilities of Southeast Asian countries in addressing emerging forms of organized online fraud and cybercrime.

UNODC Validation Workshop for Cybercrime Legal Study

The United Nations Office on Drugs and Crime (UNODC) organized the UNODC Validation Workshop for Cybercrime Legal Study, held from 28–30 January 2025 in Tokyo, Japan. The workshop was attended by representatives from several Southeast Asian countries, including Indonesia, Malaysia, Philippines, Thailand, Vietnam, Laos, and Cambodia. The activity was organized with the support of the Government of Japan as part of a project titled "Advancing the Capabilities of Southeast Asian States to Counter New Forms of Organized Online Fraud and Cybercrime," funded by the Japanese government. The workshop discussions aimed to foster participation and collaboration among ministries and agencies in Indonesia as well as international partners, particularly in strengthening cooperation in cybercrime investigations.

Online Training on the Covert Engagement Course by the Jakarta Centre for Law Enforcement Cooperation (JCLEC)

The participation of the Badan Siber dan Sandi Negara (BSSN) in the Online Covert Engagement Course (OCEC) at the Jakarta Centre for Law Enforcement Cooperation (JCLEC), held from 16–20 June 2025 in Semarang, Indonesia, was part of a strategic effort to strengthen BSSN's institutional capacity in cyber investigations, particularly in techniques related to online covert engagement. This training was relevant in the context of enhancing the technical and tactical capabilities of BSSN personnel in identifying, monitoring, and responding to potential covert cyber threats, as well as supporting early detection functions against illegal activities in the digital space.

2025 APISC Security Training Course

The 2025 APISC Security Training Course is a program organized by the Asia Pacific Information Security Center (APISC) in collaboration with the Korean Computer Emergency Response Team Coordination Center (KrCERT/CC) and the Korea Internet & Security Agency (KISA) in Seoul, South Korea, from 24–30 August 2025. The training was designed to enhance professional competencies in cyber incident handling and was divided into two training classes, namely the Basic Course and the Advanced Course. The Basic Course follows the TRANSITS I curriculum, which focuses on strengthening technical, organizational, communication, and legal aspects in CSIRT operations.

The 2nd ASEAN Regional Computer Emergency Response Team Task Force Meeting

The 2nd ASEAN Regional CERT Task Force Meeting was held on 26 August 2025 at the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in Singapore. The meeting was initiated by the National Cyber Security Agency of Malaysia as the ASEAN CERT Coordinator for the 2024/2025 period. Indonesia's participation was expected to strengthen its national position in regional cooperation; present strategic initiatives related to the harmonization of CERT standards and build collaborative networks that support cross-border incident response.

OIC-CERT Board Meeting & FDC Summit

The OIC-CERT Board Meeting, held in Cairo, Egypt from 28 April to 2 May 2025, was a closed meeting attended by representatives from Indonesia, Oman, Malaysia, Azerbaijan, United Arab Emirates, and Egypt. During the meeting, discussions covered activity reports across each KPI pillar, the financial report from the secretariat, implementation challenges, and projections for future activities, as well as plans to revise the operational manual.

OIC-CERT Board Meeting No. 4/2025 & Regional Cybersecurity Week

This activity was held in Rabat, Morocco from 15 to 19 September 2025. The Regional Cybersecurity Week 2025 is one of the largest cross-regional cybersecurity conferences, organized by the Regional Cybersecurity Center (RCC) Oman in collaboration with the General Directorate for Information Systems Security Morocco (DGSSI). The event carried the theme "Digital Sovereignty for Sustainable Economic Development." The main objective of Regional Cybersecurity Week is to bring together regional and global cybersecurity stakeholders to strengthen cybersecurity capacity and cooperation at the regional level.

AJCCBC Ensuring Cyber Resilience through Pre-Incident Response and Audit Activities Online 2025

This activity was organized by the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in collaboration with the British Embassy Jakarta. The training took place from 18–21 March 2025 with the theme "Ensuring Cyber Resilience through Pre-Incident Response and Audit Activities." The training provided explanations and discussions on key cybersecurity concepts, including understanding the attack surface, protection of devices, networks, and personnel, vulnerability management, audit, and assurance, as well as implementation exercises and group work.

Workshop Cyber security Resiliency and Digital Safety

This activity was organized by the Shadowserver Foundation on 15 May 2025 at the British Embassy Jakarta in Jakarta, Indonesia. The event was held as part of the implementation of the Indo Pacific Cyber Programme, an initiative launched by the Government of the United Kingdom. The workshop aimed to strengthen participants' understanding of attack surface detection, the misuse of network assets by threat actors, and the importance of coordination among stakeholders in receiving and responding to alerts from vendors.

ASCCE-MS Cybersecurity Roundtable on AI Singapura

The Regional Cybersecurity Week 2025 was held in Rabat, Morocco from 15 to 19 September 2025. This event is one of the largest cross-regional cybersecurity conferences, organized by the Regional Cybersecurity Center (RCC) in Oman in collaboration with the General Directorate for Information Systems Security Morocco (DGSSI) of Morocco, under the theme "Digital Sovereignty for Sustainable Economic Development." The main objective of Regional Cybersecurity Week is to bring together regional and global cybersecurity stakeholders to strengthen cybersecurity capacity and cooperation at the regional level.

Cybersecurity Expert Training Course

The Cybersecurity Expert Training Course program is organized by the National IT Industry Promotion Agency (NIPA) in collaboration with the Korea Internet & Security Agency (KISA) as part of the implementation of cooperation between Indonesia and South Korea in the field of cybersecurity. The program will be held from 25 August to 3 September 2025 in Seoul, South Korea, and will invite representatives from various international organizations involved in cybersecurity. The program aims to enhance human resource capacity, strengthen global collaboration networks, and reinforce cooperation between Indonesia and countries in Asia, particularly South Korea. It will also discuss topics such as strategies for improving cyber resilience, strengthening cybersecurity governance and human resources, and the development of artificial intelligence in the cyber domain.

JP-US-EU Industrial Control Systems Cybersecurity Week
This program is a training initiative focused on enhancing Industrial Control Systems (ICS) cybersecurity capacity in the Indo-Pacific region. The program was held from 18–21 November 2025 in Tokyo, Japan, and was organized by Japan, the United States, and the European Union. The program included various activities such as seminars, workshops, hands-on training, and visits to ICS security training facilities in Japan. In addition, the program featured participant presentations, sectoral discussions, and networking sessions aimed at encouraging regional collaboration and knowledge exchange among cybersecurity practitioners and experts from various countries.

2026 PLANNED ACTIVITIES

As part of its active contribution to OIC-CERT and in line with its role as Deputy Chair, NCCA will lead two key programs throughout Q2 and Q3 of 2026, aligned with the following Key Performance Indicators (KPIs):

KPI 1: Establish Specialized Cybersecurity Training Programs for OIC-CERT Members
NCCA will organize Cybersecurity Workshop Programs, to be held once a year, aimed at enhancing the technical capabilities of OIC-CERT members. These workshops will focus on hands-on and in-depth topics that are highly relevant to current cybersecurity threats. Proposed alternative themes include:

- Log Analysis Training: From Raw Data to Threat Insights: Advanced Log Analysis Techniques.

KPI 2: Establish Cybersecurity Capacity Building Awareness Programs for OIC-CERT Members
To strengthen cybersecurity awareness and strategic readiness, NCCA will also lead Awareness Programs, conducted three times a year. These programs aim to broaden understanding of policy, governance, and emerging threats among OIC-CERT stakeholders. Proposed alternative themes include:

- AI Security: The Dark Side of AI: Weaponized AI and Cybersecurity Risks.
- Cyber Diplomacy: Improving Global Cybersecurity Index: Policy, Diplomacy, and Strategy.
- Quantum Cryptography: Post-Quantum Cryptography: Preparing for the Future of Secure Communications.

CONCLUSION

In conclusion, the total anomaly traffic in Indonesia during 2025 was 5,515,394,886 anomalies, with the highest type of anomaly traffic being Mirai Botnet with a total of 2,124,835,234 activities. The Mirai Botnet is one type of botnet that targets Internet of Things (IoT) devices and is designed to carry out Distributed Denial of Service (DDoS) attacks on websites or online services, resulting in disruption or downtime. In 2025, there were 39,685,439 Advanced Persistent Threat (APT) activities, 13,915,440 ransomware activities, and 246,288,299 phishing activities. BSSN has sent 2,855 incident indication notifications to stakeholders, with the most common type of notification being Data Breach. In cases of web defacement, 4,433 cases were found targeting several domains. BSSN has published 144 security advisories. One of the top national CVEs

based on the Common Vulnerability Scoring System (CVSS) score with a Critical impact level is CVE-2020-0796 on Microsoft Windows SMBv3, which allows threat actors to execute commands with system access rights, install or run malware, modify or delete data, and create new user accounts with administrative rights.

Based on BSSN analysis, several potential technical cyber threats are predicted to emerge in 2026. Potential technical cyber threats include AI Driven Cyber Attack, Quantum Computing Related Cyber Threat, Cybercriminal Ransomware-as-a-Service, Advanced Persistent Threat (APT), Phishing, Stolen Credential, Web Defacement, Malware, and Distributed Denial of Service (DDoS).

Id-SIRTII/CC, on behalf of Indonesia as Deputy Chair of OIC-CERT, has successfully delivered and completed 100% of the 2025 KPIs under the 3rd Pillar –Cybersecurity Talent Development by organizing four specialized capacity building webinars from July to October 2025. These programs have demonstrated Indonesia's strong leadership in advancing technical, operational, and strategic cybersecurity capabilities across the OIC-CERT community and have laid a solid foundation for sustained collaboration and knowledge sharing. However, despite this success, the level of direct participation from OIC-CERT member organizations and the absence of a structured mechanism to measure knowledge uptake and impact remain key areas for improvement.

JORDAN

NATIONAL CYBER SECURITY CENTRE (NCSC)

المركز الوطني للأمن السيبراني
National Cyber Security Center

HIGHLIGHTS OF 2025

Summary of Major Activities

During 2025, Jordan witnessed a significant advancement in its national cybersecurity ecosystem, led by the National Cyber Security Centre (NCSC). Efforts focused on strengthening national readiness, enhancing institutional capabilities, expanding international cooperation, and improving global performance indicators.

Key achievements included:

- Expansion of SOC infrastructure and object storage.
- Complete replacement of the legacy monitoring solution with new one.
- Migration of over 100 government entities to the monitoring solution.
- Deployment of endpoint protection tools across government entities.
- Migration and tuning of government firewalls to Next-Generation firewalls.
- Deployment of Network Detection and Response (NDR).
- Implementation of content filtering solution.
- DNS Security solution project.
- Launch of AI-enabled monitoring capabilities.
- Big Data (Data Lake) project implementation.
- SOC infrastructure and object storage expansion
- Rolled out a new endpoint protection solution.
- Cyber Security Law Amendment of 2025.
  - Amendments to the Cyber Security Law are currently in progress to ensure continued alignment with emerging technologies and evolving cyber threats.

Achievements

The National Cyber Security Centre (NCSC) is the national authority responsible for strengthening and protecting cyber security in the Hashemite Kingdom of Jordan. It leads national efforts in prevention, detection, and response to cyber threats to safeguard critical digital infrastructure and national digital security.

The Centre develops national cybersecurity policies and standards, builds institutional and human capacity, enhances awareness, and coordinates international and national cooperation initiatives.

- Complete migration of over 100 Government entities from the legacy monitoring solution to our new security monitoring solution.
- Migration 76 entities server's endpoint protection solution across most government entities
- Tunning and optimization of Government entity firewalls
- Deploy NDR (Network Detection and response)
- Deployed a proxy and content filtering solution from next generation proxy solution including manager and enforcement module
- DNS Security solution project

ABOUT ORGANIZATION

The National Cyber Security Center of Jordan is the national authority responsible for strengthening and safeguarding cybersecurity across the Hashemite Kingdom of Jordan. The Center leads national efforts in preventing, detecting, and responding to cyber threats, ensuring the protection of critical information infrastructure and enhancing national digital resilience.

The Center is responsible for developing and implementing national cybersecurity policies, standards, and frameworks, as well as building institutional and human capacities. It also plays a key role in raising cybersecurity awareness, coordinating with national stakeholders, and fostering international cooperation through information sharing and strategic partnerships.

Through its strategic initiatives and operational capabilities, the Center supports government entities and critical sectors in managing cyber risks, strengthening incident response readiness, and promoting a proactive and resilient cybersecurity ecosystem at the national level.

ACTIVITIES & OPERATION

Scope and definitions

The Centre's scope includes:

- Protection of national cyberspace.
- Security Operations Centre (SOC).
- SOC Support.
- Vulnerability Management.
- Threat Hunting.
- Incident Handling and Reporting.
- Threat Intelligence sharing.

- Support to critical infrastructure sectors.
- Cyber security controls for critical infrastructure were developed and deployed. These controls aim to provide vital institutions across various sectors with the necessary safeguards to enhance their cyber security systems
- Conducted a cyber drill as part of the C8 2025 Cyber Security Advancement, Innovation, and Technology Conference, with participation from a range of organizations across various critical sectors.
- Conducted a cyber security assessment and remediation of both the IT and OT networks in several critical infrastructure organizations.
- Conducted a simulated cyber-attack exercise (TTX) in the energy sector. The exercise simulated a cyber-attack scenario targeting an energy organization, aiming to test and enhance sound decision-making and effective crisis response capabilities.
- Launched the Sectorial Cyber Incident Response Team (CERT) project across several different sectors.
- CTIA Program (46 participants)
- Cyber Threat Intelligence sharing:
  - The national cyber threat intelligence function served as a critical pillar of Jordan's proactive defense, delivering high-fidelity, context-rich intelligence that optimized threat prioritization and detection workflows.
  - The cyber threat Intelligence successfully integrated advanced intelligence into the national security stack, enhancing detection and incident response through deep-dive analysis of adversary vectors and deliver enriched indicators of compromise (IOCs) and TTPs to our stakeholders.
  - As a core pillar of the national cybersecurity strategy, the national TIP Project is being orchestrated to transform threat intelligence exchange across all critical infrastructure sectors.
  - This project replaces fragmented intelligence silos with a centralized, high-performance national platform, enabling seamless intelligence synchronization and the proactive disruption of sophisticated global cyber adversaries. By streamlining the full intelligence lifecycle from automated ingestion and normalization to high-fidelity enrichment and dissemination the initiative empowers national stakeholders with actionable, decision-grade intelligence. This supports a decisive shift from reactive defense to a unified, proactive cybersecurity posture, ultimately strengthening the resilience and sovereignty of the Kingdom's digital ecosystem.

Incident handling reports

In 2025, NCSC enhanced its national incident response capabilities through:

- Early detection and continuous monitoring.
- Advanced technical analysis and digital forensics.
- National coordination mechanisms.
- Migration of entities to monitoring solution.
- Deployment of XDR/EDR across entities.
- Optimization of government firewalls.
- Deployment of NDR capabilities.
- Implementation of DNS Security.
- Expansion of SOC infrastructure.

These efforts significantly improved response time and reduced operational impact across critical sectors.

	Q1	Q2	Q3	Q4
The Number of incident response operations	22%	21%	32%	24%
The Number of evidence collected by the Incident response	13%	16%	41%	31%
The number of Malware Analysis	10%	11%	46%	33%

Abuse statistics

Category	Total number of incidents
Malware	22%
Others	26%
Phishing Email	12%
APT	6%
Data Leak	8%
Web shell	8%
Ransomware	4%
Reconnaissance	4%
Password Attacks	3%
Misconfiguration / Default configuration	2%
Denial Of Service	1%
Vulnerability Exploitation	1%
Website Hacked	1%
Intrusion Attempts	1%
Crypto Mining / Crypto jacking	1%
SQL Injection	0%
Policy Violation	0.00327869
Data Breach	0.00327869

Category	Number of Incidents
Transportation	5%
Government Services	27%
Industry and Trade	27%
Education	15%
Finance and Banking	1%
Health	7%

Category	Total number of incidents
Communications and Information Technology	10%
Agriculture Water and Environment	3%
Energy	6%
Défense and Security	0%

Publications

Periodic threat intelligence reports, technical advisories, risk assessment reports, awareness materials, and national cyber security guidelines.

New Services

- National Threat Intelligence Platform (TIP)
- National Sandbox Services
- AI-powered SOC capabilities
- Content Filtering
- Big Data (Data Lake) Project
- Advanced Incident Response Support Services

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- Four Cyber Nashama camps have been completed, with a total of 105 graduates.
- Three cohorts of the Masar field training program for university students have been successfully completed, with a total of 676 trainees.
- A total of 127 school students from five schools across the Kingdom were trained on Capture The Flag (CTF) challenges.
- A School CTF competition was organized, with 278 participants representing 42 schools.
- A University CTF competition was held, with 296 participants from 17 universities.
- A total of 45 diverse awareness workshops were conducted for schools, universities, and public and private sector institutions, benefiting 1,662 participants.
- The "Cyber Toolkit" program was implemented, training 29 teachers to deliver cybersecurity awareness to students during activity periods.
- The "Tahseen" program was implemented to train legal professionals in cybersecurity, with 25 participants from 13 government institutions and ministries.
- Ten entities were trained in person on the "Wa'i" platform.
- Four digital cybersecurity awareness campaigns were launched: "Digital Tip," "You Are the Hero," "Cyber Crescent," and "Communicate Safely."

- One podcast episode was recorded for the "Cyber Story" program; however, it has not yet been published.
- The C8 Cybersecurity Summit was successfully held.
- A specialized training course titled "Associate Cyber Threat Intelligence Analyst (ACTIA)" was conducted for government institutions, benefiting 46 participants.
- The National Cybersecurity Center won the Best Film Award for a production on the safe use of artificial intelligence applications in cybersecurity.

Participation in international conferences including:

- CYBERUK 2025
- Black Hat Middle East & Africa
- Arab cyber security Ministers Council
- Regional and international cyber exercises
- Women in cyber security Programs
- CRI Initiative events
- Participation in the Gulf-UK Women's Cybersecurity Fellowship Program in Riyadh, Saudi Arabia
- Participation in Women Cyberspace and Digital Policy (CDP) in New York City, USA
- Participation in the CYBERUK.2025 Conference in Manchester, UK
- Participation in the Cybersecurity and Sustainable Development of Defense Technologies event in Thailand
- Participation in the Regional Conference on Immediate Response to Cyber Attacks 2025 in Tunis, Tunisia
- Participation in the International Conference on Combating Crimes Committed Using Information and Communication Technologies in St. Petersburg
- Attendance at the Seminar on Information Security Management for Belt and Road Countries
- Participation in the Seminar on Cybersecurity in ASEAN Central Asia
- Participation in the CRI Initiative and attendance at Cyber Week in South Korea
- Attendance at the CRI Global Malware Initiative Summit in Singapore
- Participation in the First Arab Cyber Exercise in Qatar
- Participation in the CYBERQ 2025 Conference on Security in the Quantum Age in the UAE
- Attendance at the BACKHAT Middle East event &Africa 2025
- Attending the Arab International Cybersecurity Conference and Exhibition (AICO 2025)
- Participating in the second session of the Arab Cybersecurity Ministers Council
- Participating in the Integrated Cybersecurity for Safer Digital Words training program
- Attending the Regional Cybersecurity Week events in Rabat

PLANNED ACTIVITIES 2026

- S Next-Generation AI-powered SOC.
- Sectoral Distributed SOC.
- SOC Optimization & Maturity Project.
- Full deployment of National Sandbox Services.

- Expansion of international partnerships.
- Improvement in Global Cyber security Index rankings.
- Complete the implementation of the Jordanian National Cybersecurity Framework for the remaining government institutions and departments.
- Activate the GRC platform to monitor the implementation of the Framework in government institutions and departments.
- Build audit and compliance capabilities.
- Finalize the implementation of projects related to establishing sectoral response teams.
- Establish controls for operational systems (OT) and Internet of Things (IoT) systems.
- Conduct a national cyber security exercise involving various sectors, encompassing both administrative and technical aspects.
- Develop a data classification and sensitivity assessment project for the National Cyber security Center.
- Review and update policies.
- Review and update the Jordanian National cyber security Framework.
- The implementation of the national threat intelligence platform (NTIP) is being orchestrated to transform threat intelligence exchange across all sectors by establishing a centralized, high-performance national platform, enabling proactive disruption of sophisticated global cyber adversaries

CONCLUSION

In 2025, Jordan continued its efforts to strengthen national cybersecurity, achieving significant progress in cybersecurity maturity. The Kingdom was classified as a "Role Model" in the Global Cybersecurity Index (GCI), according to the latest report issued by the International Telecommunication Union (ITU). Additionally, Jordan's score in the National Cyber Security Index (NCSI) improved to 85. These achievements included strengthening institutional governance, expanding strategic international partnerships, and enhancing national resilience and digital trust. The National Cybersecurity Center also continued to develop policies and regulatory frameworks, improve incident response capabilities, and expand national capacity-building programs, contributing to higher readiness and stronger protection of the Kingdom's digital infrastructure.

Looking ahead to 2026, the National Cybersecurity Center aims to achieve further progress by launching innovative initiatives and adopting advanced, intelligent cybersecurity solutions. The Center will continue to invest in developing national talent and strengthening international cooperation, with the goal of enhancing information security, increasing the resilience of digital systems, and building a safer and more sustainable cyber environment.


المركز الوطني للأمن السيبراني
National Cyber Security Center


IT SECURITY C&T


C8 2025


المركز الوطني للأمن السيبراني
National Cyber Security Center


أنت
البطل
اطلب من والديك
تحديث كلمات المرور الخاصة بك باستمرار
واستخدام كلمات مرور قوية ومعقدة
المركز الوطني للأمن السيبراني
National Cyber Security Center

JORDAN

JO-FINCERT

فريق الاستجابة لحوادث الأمن السيبراني
للقطاع المالي والمصرفي

Jo FinCERT

HIGHLIGHTS OF 2025

Summary of Major Activities

Capacity Building and Training:

1. Delivered the second edition of the Cybersecurity Bootcamp as a key sector program, expanding it into a structured, multi-level training with diverse technical tracks aligned with sector needs.
2. Conducted advanced Tabletop Exercises (TTX) for non-banking financial institutions and a large-scale Cyber Drill for the banking sector, simulating real-world cyber incidents. Improved response readiness, coordination, and decision-making under pressure.
3. JoPACC Hackathon: An innovation-driven hackathon organized in collaboration with JoPACC to engage talent in developing creative cybersecurity and payment-related solutions for the financial sector.

Awareness:

1. Launched a national cybersecurity awareness campaign using multiple media platforms to address cyber threats and fraud methods. Increased public awareness and promoted safe digital practices across the Kingdom.
2. Conducted more than 30 awareness sessions across Jordan, reaching different segments of society. Provided practical guidance to help individuals identify and prevent cyber risks.
3. Awareness Creative Video Competition: An initiative encouraging participants to produce creative content that promotes cybersecurity awareness and safe digital practices across the community.

Cybersecurity Services for the Financial Sector:

1. Enhanced Threat Intelligence and Automated Intelligence Sharing: Advanced commercial threat intelligence feeds along with strategic integration with a collaborating international organization were successfully integrated with our internal threat hunting and analytical processes significantly improving the early detection of emerging threats and enabling more proactive defence mechanisms across the sector. In parallel, a customized orchestration workflow was developed and implemented to automate the sharing of threat intelligence with the financial sector across multiple use cases, ensuring that Indicators of Compromise (IOCs) are consistently high-confidence, contextually enriched, and supported by accurate threat scoring.

2. Email Security: The solution was expanded to cover both the banking and non-banking sectors to reduce the risk of successful email spoofing attacks. This initiative focused on strengthening email authentication mechanisms—SPF, DKIM, and DMARC—in alignment with industry best practices, while enhancing visibility into authorized senders and streamlining the analysis of both aggregate and forensic reports.
3. Vulnerability sectoral scanners: A sector-wide vulnerability scanner program was introduced to systematically identify, assess, and mitigate security vulnerabilities, thereby reducing overall cyber risk exposure.
4. Satellite Internet for Business Continuity: Satellite internet connectivity will be deployed in 2026 as a backup communication channel for critical services. This ensures operational continuity and resilience during network disruptions or outages.
5. Deployment of the GRC and the Cyber Map Platform: A Governance, Risk, and Compliance (GRC) platform, along with a Cyber Map, was deployed to enhance risk visibility. These tools support informed decision-making and provide a comprehensive overview of the sector's cybersecurity posture.

Framework and Strategy Development:

1. Issued the regulatory framework for the use of artificial intelligence in the Jordanian banking sector, ensuring safe and responsible adoption.
2. Launched the sectoral roadmap for the transition to quantum-resistant cryptography (QRC 2025), preparing the sector for future risks.
3. Conducted cybersecurity maturity assessments and updated the banking sector cybersecurity framework to Version 2, aligning with global standards.

Achievements

- Launched the national strategic project for a unified digital financial identity, supporting secure digital transformation and financial inclusion.
- Delivered comprehensive cybersecurity assessments for more than 20 institutions across all regulated sectors, strengthen baseline security posture and improving overall security readiness.

ABOUT ORGANIZATION

The Jordan Financial Computer Emergency Response Team (Jo-FinCERT), established under the Central Bank of Jordan (CBJ), plays a crucial role in enhancing the cybersecurity resilience of Jordan's financial and banking sector. As cyber threats continue to grow in complexity and frequency, Jo-FinCERT operates as a central hub for threat intelligence, incident response, and sector-wide collaboration, ensuring a proactive and coordinated approach to cybersecurity. The initiative aligns with global best practices and follows internationally recognized cybersecurity frameworks to strengthen Jordan financial institutions' defences against cyberattacks. These efforts contribute to Jordan's financial stability, economic security, and digital trust, reinforcing the CBJ's commitment to safeguarding Jordan's financial ecosystem. By fostering a culture of

cybersecurity resilience, Jo-FinCERT not only protects critical financial infrastructure but also ensures continued confidence in Jordan's financial sector in an increasingly digital world.

ACTIVITIES & OPERATION

Scope and definitions

- Provide shared cybersecurity services across the financial sector
- Coordinate incident response and handling
- Conduct regular on-site and remote cybersecurity assessments
- Collaborate with local and international stakeholders
- Deliver capacity building and specialized training programs for the financial sector
- Promote cybersecurity awareness for the financial sector and the wider community

Threat Intelligence, Advisory, Crimeware and Threat Hunting Reports

Throughout 2025, comprehensive threat intelligence, advisory, crimeware, and threat hunting reporting capabilities were enhanced to support the financial sector. This included the production and dissemination of actionable intelligence reports, strategic and tactical advisories, and proactive threat hunting outputs. These reports enabled entities to understand the evolving threat landscape, identify potential risks, and implement timely mitigation measures. Additionally, threat hunting activities were conducted using enriched intelligence sources and advanced analytics to detect hidden threats and previously unknown attack patterns within the environment.

Dark and Deep Web Monitoring

Dedicated monitoring of dark and deep web sources was conducted through a combination of manual analysis and specialized monitoring systems to identify potential threats targeting the financial sector. This included tracking leaked credentials, compromised financial data (Cards Breach, Payment Fraud), sensitive documents, and emerging threat actor activities. The insights gathered were analysed and shared with relevant stakeholders to support early warning and proactive defence. This capability also contributed to identifying planned cyberattacks, such as data breaches or distributed denial-of-service (DDoS) campaigns, enabling pre-emptive action to mitigate risks.

Publication(s)

- Issued Artificial Intelligence (AI) Guidelines for the Banking Sector
- Published Post-Quantum Cryptography (PQC) Guidelines

New service(s)

- Secure Access Service Edge (SASE): A private cloud-based architecture combining networking and security functions to provide secure and scalable access to applications and services for the non-banking sector.
- GRC Platform and Cyber Map: Tools deployed to enhance risk visibility, centralize compliance management, and support data-driven decision-making.
- Crimeware Reports, and APT Profiling: Tool deployed to provide actionable, timely intelligence on malware campaigns, financial threats, and tools used by criminals.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

Jordan FinCERT has led and organized several key cybersecurity events to enhance financial sector resilience and strengthen industry-wide collaboration, including:

- Delivered the Financial Security Bootcamp 2025 as a multi-track training program, including technical certifications, a CISO program, and a penetration testing track.
- Organized the CISO Forum, bringing together cybersecurity leaders from the banking sector to discuss challenges and share best practices.
- Conducted Tabletop Exercises (TTX) and Cyber Drills to simulate cyber incidents and improve response readiness.

Events involvement

Jordan FinCERT has actively participated in key national events to raise cybersecurity awareness about the latest threats and best practices for addressing them and innovations within Jordan's Financial Sector:

- Served as the main sponsor of the C8 Summit 2025.
- Concluded the DISIFI challenge in collaboration with JoPACC, including announcing the winners.

2026 PLANNED ACTIVITIES

Academy

A specialized Cybersecurity Academy will be established to qualify and train professionals in the field of cybersecurity, enhancing skills, knowledge, and practical capabilities in line with international standards.Summit
A regional and international summit will be organized, bringing together the financial sector, banking institutions, and central banks to discuss emerging cybersecurity challenges, share best practices, and strengthen cooperation.

Campaign
A comprehensive awareness campaign will be launched to promote cybersecurity culture, educate stakeholders on risks and safe practices, and enhance overall digital security awareness across targeted audiences.

Collaboration
Strategic collaborations will be developed with local and international partners to exchange expertise, support capacity building, and foster innovation in cybersecurity within the financial sector.

CONCLUSION

In 2025, Jordan FinCERT made strong progress in strengthening the Kingdom's financial cybersecurity sector, supported by clear strategy, effective international partnerships, and the use of advanced security frameworks. By improving national policies, enhancing incident response capabilities, and delivering impactful capacity-building programs, these efforts have further reinforced Jordan's position as a regional leader in cyber resilience and preparedness. In addition, Jordan FinCERT kept pace with emerging cybersecurity trends, including the use of artificial intelligence in threat detection, zero-trust approaches, and advanced threat intelligence, ensuring that the financial sector remains flexible and ready to face evolving risks.

Looking ahead to 2026, Jordan FinCERT remains committed to advancing cybersecurity through innovation, proactive threat management, and continuous development of skilled professionals. By staying aligned with global developments and anticipating future challenges, it will continue to strengthen its capabilities and support a more secure, adaptive, and resilient financial sector.

Figure 1: The Campaign Launch Ceremony

Figure 2: The Annual CISO Meeting

Figure 3 Cyber Drill & TTX Exercis

REPUBLIC OF KAZAKHSTAN

KZ-CERT
(NATIONAL COMPUTER EMERGENCY RESPONSE TEAM OF KAZAKHSTAN)

KZ CERT

HIGHLIGHTS OF 2025

Awareness-raising

One of the key areas of our work is raising awareness on cyber threats and promoting a culture of information security among various segments of the population. In 2025, our organization carried out educational events and cyber drills for employees of government agencies in Kazakhstan, the quasi-government sector, critical information and communication infrastructure (CICO) facilities, and Security Operations Centers. As part of these events, we address key issues of digital security, including:

- Cyber threats, attacks, and countermeasures – an overview of contemporary threats, attack methods, and effective defense strategies;
- Data protection in the digital reality – approaches to ensuring the security of personal and professional information in the context of digital transformation;
- Cyber hygiene basics and common internet fraud schemes – recommendations for safe online behavior and common scams;
- Digital defense: protection from cyberattacks, basics for public servants – practical advice on information security for government employees;
- Cybercrime: how to avoid digital fraud – strategies for protection against online threats and scammers;
- Cyber hygiene guide for schools – safe digital practices adapted for teenagers;
- Safe internet for children – educating children and parents on the basics of internet safety;
- The secrets of the internet: safety in the digital age – how to protect privacy and minimize digital risks;
- Key aspects of information security – understanding threats and the necessary protective measures for every user.

Internal Operations

In 2025, within this initiative, KZ-CERT implemented a series of events aimed at increasing digital literacy, protecting against cyber threats, and strengthening information security in Kazakhstan.

As part of the ongoing activities to cover the cybersecurity issues in our country, the meetings that involve Kazakhstan's government agencies and Security Operations Centers have been held to discuss matters related to enhancing the level of information security in these organizations that play a significant role in domestic policy.

ABOUT ORGANIZATION

Introduction

KZ-CERT is a single center for the users of national information systems and the Internet segment of Kazakhstan which provides collection and analysis of cyber incident reports as well as consultative and technical assistance to kazakhstani users in preventing of cyber threats.

Establishment

KZ-CERT was established in 2011 on the basis of the "Center for Technical Support and Analysis in Telecommunications" republican state enterprise on the right of economic management.

On January 28th, 2013, the government of Kazakhstan adopted a decree to rename the "Center for Technical Support and Analysis in Telecommunications" RSE on REM as the "State Technical Service" RSE on REM. Eventually, in 2020, the "State Technical Service" RSE on REM had undergone its final reformation into the "State Technical Service" joint-stock company (JSC STS) by another governmental decree.

In 2017, the National Coordination Center for Information Security (NCCIS) was established as a structural unit of the JSC STS. It combines the operation of both KZ-CERT and the Government SOC.

Resources

The National Coordination Center for Information Security (NCCIS), which is a structural subdivision of STS JSC, currently employs more than 80 people of various profiles. KZ-CERT, in turn, as a functioning unit of NCCIS, comprises around 20 employees.

ACTIVITIES & OPERATION

Incident handling reports

In 2025, KZ-CERT has handled over 61 thousand cybersecurity incidents. The majority of incidents are associated with the creation and distribution of malware. Figure 1 shows a more detailed information on their types.

Figure 1. 2025 incidents statistics. Source: https://cert.gov.kz/

Operations: 2025 Cybersecurity incidents and threats

As a National Computer Emergency Response Team of Kazakhstan, KZ-CERT continuously monitor, analyze, and respond to cybersecurity incidents and threats across the country. The following section provides an overview of the significant incidents and emerging threats identified during the reporting period.

Botnet

At the beginning of the current year, numerous events associated with the Phorpiex botnet – one of the most persistent and active cyber threats currently observed (accounting for approximately 90% of the total number of detected botnets) – were identified within the infrastructure of JSC "STS" This malware is commonly used for cryptocurrency wallet theft, spam distribution, sextortion campaigns, and the propagation of ransomware According to international and internal intelligence sources, more than 1000 IP addresses located in Kazakhstan were identified in connection with botnet activity, indicating a significant level of infection within the national network segment.

In several public sector organizations, malicious files (for example, "voldriver.exe") associated with a new variation of the botnet – Twizt – were detected This variant utilizes a peer-to-peer architecture and is capable of operating without centralized command-and-control infrastructure, which significantly increases its resilience and complicates detection and mitigation efforts.

The continued activity of botnets may be attributed to the compromise of new information systems as well as the ongoing evolution of command-and-control mechanisms and management algorithms for infected devices This situation highlights the need to strengthen protective measures, improve the level of cybersecurity awareness among public sector personnel, and implement additional monitoring and incident response mechanisms.

Countering botnet threats such as Phorpiex and its Twizt modification requires a multilayered approach to protecting information infrastructure It is necessary to ensure monitoring coverage across all network ports and protocols through attack detection and prevention solutions, implement behavioral traffic analysis, and extend signature-based detection capabilities beyond standard rule sets Effective measures include the deployment of SIEM platforms as well as the timely acquisition and integration of Indicators of Compromise (IoC) from trusted intelligence sources Network segmentation should be enforced, routing from compromised nodes should be restricted, and connections to peer-to-peer networks commonly utilized by malware should be blocked.

It is also necessary to review and update existing security policies, maintain up-to-date antivirus protection, and train personnel to identify indicators of anomalous network activity. Regular security audits of internal infrastructure are recommended in order to detect potential involvement in botnet activity.

In addition, particular attention should be given to remote workplaces and workstations generating a high volume of outbound requests that may indicate signs of compromise.

Data breaches

During 2025, data breaches became one of the most significant and widespread information security threats. Multiple large-scale incidents involving the compromise of sensitive information affecting both government institutions and private organizations were identified across various online resources. The total volume of compromised data amounts to tens of millions of records. In several cases, the data became publicly accessible through open sources or was distributed via messaging platforms and specialized forums.

Organization in the transport sector

An incident involving the potential unauthorized transfer of internal documents was identified in an organization operating in the transport sector. Although no direct evidence of large-scale data exfiltration to the Internet was obtained, analysis of user directories, graphical files, and system artifacts (including registry data and USB device connection logs) revealed indications of possible involvement by certain employees. One document was subsequently published in a Telegram channel and further disseminated online, suggesting the possibility of a targeted data leak.

Organization in the emergency medical services sector

A database leak involving approximately 800,000 records associated with an information system used in emergency medical services was identified. An open web resource contained links to official web resources of the system as well as information regarding the database structure, including records of ambulance stations. As proof of access, the threat actors published samples of 10,000 records for each city, indicating that they possessed full access to the dataset.

Organization in the e-commerce and digital services sector

As a result of the compromise of a web resource belonging to an organization operating in the e-commerce and digital services sector, threat actors obtained access to a substantial dataset containing approximately 4.5 million records. The leaked materials included files and databases

with various names suggesting links to telecommunications services, educational platforms, and contact data processing services. The majority of the records relate to citizens of neighboring countries, however information concerning citizens of the Republic of Kazakhstan was also identified, creating additional risks for national stakeholders.

Organization in the healthcare sector

Particular attention should be given to a large-scale data breach presumably originating from a major information system used in the healthcare sector. The dataset is estimated to contain approximately 16 million records. A similar dataset had previously appeared for sale in December 2024, which may indicate a prolonged compromise and the possibility that the same data has been repeatedly resold to different threat actors.

Organization providing financial services

An incident was recorded in which a file containing 228,682 records with personal client data belonging to a financial services organization became publicly accessible. The dataset included partially masked bank card numbers, card expiration dates, payment system identifiers, client names, cities of residence, and phone numbers. The combination of this information significantly increases the likelihood of financial fraud and targeted phishing campaigns against affected clients.

Organization in the mass media sector

A leak involving more than 5.3 million records was identified on the web resource of an organization operating in the media sector. The dataset covers the period from 2016 to 2025 and includes both internal website information and personal user data. The scale of the dataset and the extended period of data accumulation indicate a potentially significant impact associated with the future misuse of this information.

Organization in the construction sector

A leak involving approximately 294,762 records related to an organization operating in the construction sector in the Republic of Kazakhstan was also identified. Analysis indicates that the majority of the records are clearly associated with residents and organizations located within the country, as evidenced by address information and references found in regional sources. The compromise affected both contact information and data enabling the identification of individuals and organizations.

The combination of the incidents described above confirms that data breaches represent one of the most significant and relevant cybersecurity threats in the last year. The scale of compromised datasets, the diversity of affected data categories, and the involvement of both public and private organizations highlight the need to prioritize data protection measures, strengthen vulnerability monitoring processes, improve the security posture of web applications and database infrastructure, and conduct systematic efforts aimed at preventing insider threats and improving employee cybersecurity awareness.

Ransomware

During the first quarter of 2025, several incidents involving data encryption within the IT infrastructure of various organizations were recorded. Analysis indicates the use of modern ransomware families such as Mimic, as well as the abuse of built-in encryption tools including BitLocker.

Data encryption in a financial sector organization

On January 12, 2025, following a compromise of the infrastructure of a financial sector organization, several servers were encrypted using BitLocker. On January 14, a compromise of the organization's web resource was also detected, resulting in redirection to an external malicious website.

The intrusion into the infrastructure was carried out through Remote Desktop Protocol (RDP) access using an administrator account, which enabled the attackers to encrypt servers and workstations. In addition, the attackers gained access to the administrative panel of a website hosted within the corporate network. The system lacked up-to-date security patches and contained a known vulnerability in the content management system (CMS) being used. Insufficient information security controls, outdated operating systems (Windows Server 2003/2012 and Red Hat Linux 4), the absence of SIEM-based monitoring, and the lack of a structured information security policy significantly exacerbated the impact of the incident.

Data encryption in a local executive body

On April 28, 2025, numerous virtual machines were encrypted within the infrastructure of an organization, including critical services such as Active Directory (AD), DHCP, and DNS. The malware disrupted system operations and a ransom note was received. Backup copies were either unavailable or inaccessible.

The attackers gained initial access through a compromised account belonging to an employee responsible for system maintenance. Using RDP access, they penetrated the domain controller server, cleared event logs, and subsequently initiated data encryption. An additional factor that facilitated the attack was the use of an outdated and vulnerable version of a CMS deployed on one of the organization's web resources.

Data encryption in an organization in the education sector

On February 7, 2025, a ransomware incident occurred within the infrastructure of an organization operating in the education sector, resulting in disruption of the normal operation of information systems. The investigation revealed that key factors contributing to the successful attack included the absence of a formalized and implemented information security policy, the presence of open network ports, the lack of regular audits of user and administrator accounts, and improperly organized backup storage procedures, which complicated system recovery.

It was additionally determined that not all IP addresses involved were connected through the centralized Internet gateway, reducing the level of traffic visibility and increasing the infrastructure's exposure to external threats. The combination of these factors created conditions that allowed the attackers to successfully encrypt data and disrupt the integrity and availability of critical services.

EVENTS ORGANIZED & INVOLVEMENT

Activities: Events and Cyber Drills

KZ-CERT recognizes the importance of cooperation with teams and organizations that have similar competency and constituency. Therefore, our Team is always open to invitations and opportunities to participate in various events dedicated to the information security matters.

International cooperation plays a big role in establishing communications with the global IT and cybersecurity communities, circulating important information, as well as maintaining the status of a national computer emergency response team on the global stage through the participation in different international information security conferences and other events.

The Standoff at the St. Petersburg International Economic Forum (SPIEF)
In June 2025, the "Standoff" cyber range at the St. Petersburg International Economic Forum (SPIEF) in Russia hosted a cybersecurity event featuring 12 teams from various countries. The goal of the Standoff was to evaluate the cybersecurity resilience of the virtual state's infrastructure in the logistics sector by investigating simulated cyber incidents, detecting malicious activity, and responding to threats. KZ-CERT secured 1st place in the competition;

OIC-CERT Cyber Drill
In September 2025, KZ-CERT participated in the 13th Regional Arab, OIC and Africa Cyber Drill event organized by OIC-CERT as part of the 17th Annual Conference held in Rabat, Morocco. The primary goal of these drills was to enhance the capabilities in defending against cyber threats and to promote cooperation in cybersecurity across member states. KZ-CERT successfully earned 2nd place in the competition;

CyberTask Cyber Drill
As part of the 13th Regional Arab, OIC and Africa Cyber Drill and the 17th Annual Conference organized by OIC-CERT in Rabat, Morocco, KZ-CERT participated in the CyberTask Cyber Drill. The exercise focused on investigating a cyber-attack against an AI-powered automation system, analyzing SIEM logs, network traffic, and forensic evidence to trace attacker activity. KZ-CERT members achieved 1st place, demonstrating the high level of expertise and preparedness;

CyberLab (MyCERT) Cyber Drill
During the same conference, KZ-CERT also took part in the CyberLab Cyber Drill, which focused on threat hunting and monitoring on a SIEM system, providing practical experience in detecting and responding to cyber threats in real-time. KZ-CERT showcased its capabilities and secured 2nd place in the rankings;

Positive Technologies Cyber Drill
KZ-CERT participated in the Positive Technologies Cyber Drill "Compromise of Medical Data" as part of the same OIC-CERT event in Rabat, Morocco. The exercise focused on investigating and responding to simulated attacks targeting medical information systems, providing practical experience in detecting breaches and mitigating threats. KZ-CERT achieved 2nd place in the team ranking and 1st place in the individual ranking.

Equinor CTF
In November 2025, KZ-CERT successfully participated in the Equinor CTF 2025, securing an impressive 3rd place finish. Throughout the competition, our team demonstrated high-level expertise in incident response, digital forensics, and log analysis;

FIRST CTF
In June 2025, KZ-CERT competed in the 37th Annual FIRST Conference CTF, which was held in Copenhagen, Denmark, securing 14th place out of 100 teams. The primary goal of the competition was to challenge participants with a diverse range of realistic attack-and-defense scenarios, requiring the team to demonstrate versatility, rapid problem-solving, and a comprehensive understanding of the modern threat landscape.

Events involvement

KZ-CERT Team members also actively attended various international conferences and meetings to gain valuable experience, stay updated on emerging cyber threats, and learn best practices from global cybersecurity experts. The following events can be mentioned in this regard:

- The 27th Big National Forum "Infoforum-2025" in Moscow, Russia;
- The "The Field of Cybersecurity in OIC Countries: Challenges and Prospects" workshop in Islamabad, Pakistan (as a speaker);
- The OSCE Workshop on Gender Issues in Cybersecurity and ICT, organized by the Transnational Threats Department in Astana, Kazakhstan;
- The "Mobile World Congress" event in Barcelona, Spain;
- The 37th Annual FIRST Conference and 20th Annual NatCSIRT Meeting in Copenhagen, Denmark;
- The "Positive Hack Days" International Cybersecurity Festival in Moscow, Russia;
- The 10th Annual CAMP Meeting in Seoul, South Korea;
- The 3rd Cybersecurity Summit for Central Asia in Tashkent, Uzbekistan;
- The "SOC-Forum" event in Moscow, Russia;
- The 13th Regional Cybersecurity Week General Meeting and the 17th Annual OIC-CERT Conference in Rabat, Morocco.

LEBANON

LEBCSIRT

HIGHLIGHTS OF 2025

The year 2025 marked a period of significant operational maturity and expanded threat visibility for the Cybersecurity Division and its SOC operations. Despite a volatile threat landscape characterized by targeted social engineering campaigns, mobile malware proliferation, and state-affiliated cyber incidents affecting national infrastructure, the team successfully maintained 24/7 monitoring, enhanced detection capabilities, and supported multiple high-priority investigations. The following highlights capture the most impactful activities, achievements, and cyber events that defined 2025.

Note that we are still working in fragmented mode due to the situation and continuous unpredictable war in our Country. The coordination is done in very hard situation and limited means. Coordination between national SOCs and the private sector is the most important

Summary of Major Activities

In the absence of a formally established national CSIRT, the Lebanese cybersecurity landscape remains fragmented across multiple entities with overlapping or disconnected responsibilities. Recognizing this critical gap, the LebCSIRT task force has undertaken a deliberate effort to consolidate capabilities, unify processes, and recover operational coherence from fragmentation. By leveraging existing assets, including the 24/7 SOC, investigative units, forensic laboratories, and training programs. The LEBCSIRT team strives to deliver CSIRT-like functions in a decentralized yet collaborative manner. The following activities represent the core pillars of this consolidation strategy, each designed to progressively close the gap until a fully mandated CSIRT becomes operational.

- **24/7 SOC operations and managed security services:** Provided continuous (24/7) security monitoring and managed SOC services, including alert triage, investigation, escalation, and coordination with stakeholders to support timely containment and remediation.
- **Security investigations and analysis:** Conducted multiple investigations throughout 2025 to analyze security events, validate potential threats, and support incident handling and corrective actions.
- **Quarterly vulnerability assessments:** Performed vulnerability assessments on a quarterly basis to identify weaknesses, prioritize remediation, and track risk reduction over time.

- **Security training for users/employees:** Delivered awareness and operational training sessions to strengthen user readiness and improve alignment with SOC processes and incident reporting practices.
- **Investigation of cybercrime cases:** Handled cases including phishing, ransomware, and social media crimes.
- **Digital forensic analysis:** Performed forensic analysis of seized computers, mobile devices, and storage media.
- **Support for national cyber incident investigations:** Assisted investigations affecting government institutions.
- **Awareness campaigns and sessions:** Conducted multiple awareness initiatives.

Achievements

The following achievements reflect the steady operational progress of LebCSIRT, highlighting concrete improvements in monitoring capabilities, detection engineering, incident response, investigative functions, inter-agency collaboration, and capacity building, despite operating within a still-developing institutional framework:

- **Log source integration and visibility improvements:** Enhanced monitoring coverage by onboarding relevant log sources into SOC platforms, improving overall visibility.
- **Use-case creation and continuous fine-tuning:** Created and refined detection use cases and correlation rules to improve alert quality, reduce false positives, and align monitoring with the evolving threat landscape.
- **Incident response support and process maturity:** Strengthened incident response readiness through improved escalation workflows, documentation, and operational playbooks.
- **Continuous service improvement:** Maintained regular operational reporting and continuous improvement cycles to optimize SOC performance.
- **Cybercrime case investigations:** Successfully investigated multiple cybercrime cases.
- **Digital forensic capabilities:** Enhanced forensic analysis through deployment of new tools.
- **Collaboration:** Established improved collaboration mechanisms with national CERT teams.
- **Training delivery:** Provided cybersecurity awareness training for public sector organizations and internal teams.

ABOUT ORGANIZATION

Lebanon is progressively consolidating its national cybersecurity governance through a coordinated, multi-stakeholder framework known as LebCSIRT. While a formally institutionalized national CSIRT is not yet established, LebCSIRT currently functions as the national coordination mechanism for cybersecurity incident handling, inter-agency cooperation, and structured information exchange. It represents a transitional but operational governance model that enables Lebanon to maintain national cyber coordination across critical sectors.

National Coordination Framework

The national cybersecurity coordination framework is led by the National Cybersecurity Committee, with technical accompaniment from the International Telecommunication Union (ITU) and support from international development partners. This arrangement has supported the progressive establishment of foundational governance elements required for a future formal CSIRT structure.

Within this context, LebCSIRT functions as a whole-of-government coordination platform, ensuring alignment between technical, operational, regulatory, and investigative stakeholders, and enabling structured national-level cyber incident coordination.

Institutional Composition and Governance Model

LebCSIRT is structured as an interagency national mechanism bringing together key state institutions with complementary mandates across cybersecurity, national security, telecommunications, finance, and academia. Its membership includes:

- Presidency of the Council of Ministers (National Cybersecurity Committee – LEBCSIRT Task Force)
- Lebanese Armed Forces (LAF)
- Internal Security Forces (ISF)
- General Directorate of General Security (GDGS)
- OGERO
- Ministry of Telecommunications
- Telecommunications Regulatory Authority (TRA)
- Central Bank of Lebanon
- Lebanese University

This composition reflects a whole-of-government cybersecurity governance model, where cyber resilience is treated as a shared national responsibility rather than a sectoral function. It enables structured coordination between operational responders, law enforcement authorities, regulatory bodies, infrastructure operators, and academic institutions.

Role of Law Enforcement Agencies – Operational Backbone of Cybersecurity Response

Law enforcement agencies—primarily the ISF, LAF, and GDGS—form a critical operational pillar within the LebCSIRT ecosystem. Their role extends beyond traditional security enforcement to include cybercrime investigation, digital forensics, and evidentiary support for judicial processes. These agencies provide essential capabilities in:

- Investigation of cybercrime incidents, including fraud, ransomware, intrusion cases, and digital abuse
- Digital forensic acquisition, preservation, and analysis of electronic evidence
- Maintenance of chain of custody to ensure judicial admissibility of cyber evidence
- Operational support during major cyber incidents affecting government or critical infrastructure
- Coordination with technical stakeholders for attribution and incident reconstruction
- This integration of law enforcement into the national cybersecurity coordination framework ensures that technical incident response is directly linked to legal accountability mechanisms. It also strengthens Lebanon's ability to transition from incident detection to prosecution and deterrence in a structured and legally robust manner.

Civil and Institutional Stakeholders – Enabling National Cyber Resilience
Civil and institutional actors play an equally important role in strengthening Lebanon's cyber resilience. The Central Bank of Lebanon contributes to the protection and coordination of the financial sector's cybersecurity posture, ensuring alignment with national risk considerations. OGERO serves as a key national infrastructure operator, supporting the resilience of telecommunications services and acting as a critical technical stakeholder within national coordination mechanisms.

Regulatory institutions, including the Ministry of Telecommunications and the Telecommunications Regulatory Authority (TRA), provide essential governance oversight and sectoral coordination, ensuring alignment between policy, regulation, and operational implementation across the ICT ecosystem.

This civil–institutional dimension ensures that cybersecurity governance in Lebanon is not limited to security actors alone, but is embedded across essential national service providers and regulatory authorities.

Academic Integration – Lebanese University as Knowledge and Talent Pillar
The Lebanese University plays a strategic role within the LebCSIRT framework by contributing academic expertise, research capacity, and cybersecurity talent development. Its involvement reinforces the link between academic knowledge and national cybersecurity needs, ensuring a sustainable pipeline of qualified professionals.

The university supports national capability development through education, applied research, and engagement in cybersecurity-related training activities, thereby strengthening the long-term sustainability of Lebanon's cyber workforce.

Interagency Coordination Model
The LebCSIRT framework is characterized by a structured interagency coordination model that enables collaboration across technical, operational, regulatory, and investigative domains. This model facilitates information sharing, coordinated situational awareness, and aligned response actions across institutions with different mandates but shared national objectives.

Despite operating under significant national constraints, this mechanism has enabled Lebanon to maintain a functional and coherent cybersecurity coordination capability, reflecting a pragmatic and resilient governance approach.

ACTIVITIES & OPERATION

Operational activities in 2025 were structured around continuous security monitoring, incident handling, vulnerability management, and proactive threat hunting. This section details the scope of SOC operations, incident handling statistics, abuse trends across email, IPS, and web vectors, as well as the specific cyber threats observed in Lebanon. Additionally, new services introduced during the year are outlined to demonstrate capability growth.

Scope and definitions

In the absence of a formally institutionalized national CSIRT, Lebanon operates through an integrated SOC-supported national cybersecurity capability (LebCSIRT), which performs essential incident response and coordination functions in alignment with CSIRT best practices.

This 24/7 SOC-supported capability provides continuous monitoring, alert triage, investigation, escalation, and coordinated response activities. Security events are collected from integrated infrastructure and security log sources, and analyzed to detect suspicious activities and validate confirmed incidents.

For reporting purposes:

- A security event/alert refers to any observable activity or detection generated by monitored systems that may be security relevant.
- A security incident refers to a confirmed event (or series of events) that violates security policy or impacts confidentiality, integrity, or availability and requires coordinated response actions.
- Alerts are prioritized using four severity levels: Low, Moderate, High, and Critical.

Within this operational model, LebCSIRT performs CSIRT-like functions, including incident analysis, technical investigation, coordination, and support to national stakeholders. The scope includes cyber incidents such as unauthorized system access (hacking), malware-related activities, Distributed Denial-of-Service (DDoS) attacks affecting service availability, phishing and online fraud, identity theft, financial cybercrime, and social media-related threats.

LebCSIRT also supports digital evidence collection and forensic analysis in coordination with relevant national authorities, while formal legal investigation and prosecution remain under the mandate of competent law enforcement agencies.

This "build-while-operating" approach ensures continuous national cyber protection and enables Lebanon to progressively align with full CSIRT institutional maturity.

Incident handling reports

Across 2025, the SOC handled alerts on a continuous basis, performing investigations, escalating when required, and coordinating response actions and follow-up with relevant stakeholders. Total alerts handled in 2025 are as follows:

Quarter	Total	Low	Moderate	High	Critical
Q1	1,563	1	1541	20	1
Q2	792	8	768	14	2
Q3	556	54	465	36	1
Q4	347	50	280	17	0
Total alerts	**3258**	**113**	**3054**	**87**	**4**

Table 1. SOC Alerts by Severity — 2025

Operationally, the SOC activities included:

- Conducting multiple investigations to validate detections, determine scope/impact, and recommend containment and remediation actions.
- Supporting incident response through escalation, coordination, and documentation.
- Continuous improvement through use-case creation, fine-tuning, and integration/onboarding of relevant log sources.
- The Cybersecurity Division handled multiple cyber incidents reported by individuals, organizations, and government entities.

Tactic	Description
Initial Access	Attackers gain entry (e.g., phishing, exploiting public-facing apps)
Execution	Running malicious code on a system
Persistence	Staying on the system after reboot or logout
Privilege Escalation	Gaining higher-level permissions (e.g., SYSTEM or root access)
Defence Evasion	Avoiding detection (e.g., disabling antivirus, obfuscation)
Credential Access	Stealing usernames, passwords, or tokens
Discovery	Mapping the environment (e.g., scanning for services, users, files)
Lateral Movement	Moving from one system to another inside the network
Collection	Gathering data of interest
Command and Control (C2)	Communicating with external attacker-controlled servers
Exfiltration	Transferring stolen data out of the network
Impact	Causing disruption or destruction (e.g., ransomware, data wiping)

Table 2 Tactic Categorization – 2025

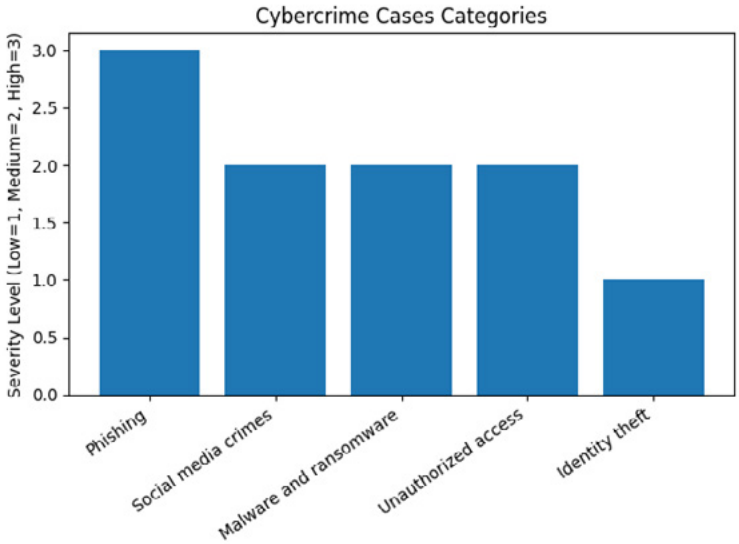


Figure 1. MITRE TACTICS Categorization – 2025

Abuse statistics

Abuse-related activity observed in the monitored environment was tracked and analyzed to identify trends and improve defensive coverage.

Alert sources were primarily driven by perimeter/security tooling and operating system telemetry, with additional contributions from DNS, endpoint/server platforms, and cloud/service logs.

Incident categories were dominated by Discovery / Network Service Scanning (42%), followed by Privilege Escalation / Sudo (33%) and Defense Evasion / File & Directory Permission Modification (21%), with smaller proportions attributed to other categories such as persistence and credential access.

Email Threat Landscape

The 2025 email threat landscape shows that legitimate mail still makes up the largest share at 47.6%, indicating that nearly half of inbound traffic is benign. However, a significant portion—over half—is malicious or unwanted. Unauthorized access and abuse accounts for 31.2%, representing the most prominent threat category and highlighting the risk of account takeover attempts and misuse of email systems. Spam and unwanted content contributes 10.3%, reflecting ongoing bulk distribution campaigns, though at a lower volume than targeted abuse. More targeted social engineering threats are seen in spoofing and identity fraud (5.9%), while malicious attachments and URLs (5%) indicate attempts to deliver payloads or phishing links. Overall, the distribution suggests a shift toward more targeted and account-focused attacks rather than purely high-volume spam, emphasizing the need for strong authentication controls and user awareness.

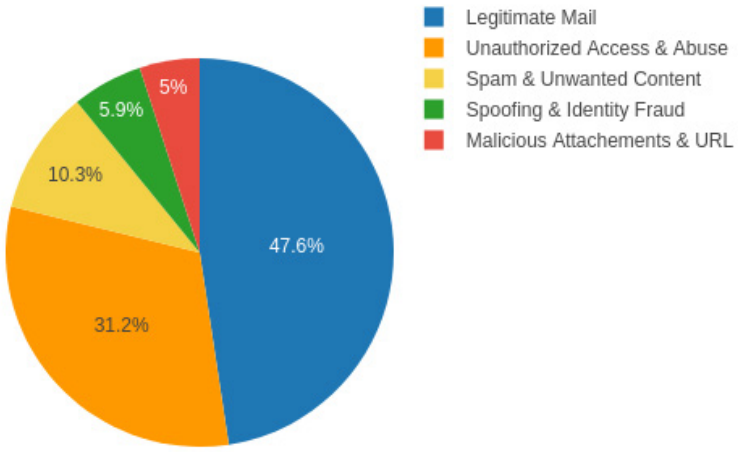


Figure 2. 2025 Email Attack Types

IPS Threat Landscape

The 2025 IPS threat landscape is heavily driven by automated scanning activity and botnet traffic, with a long tail of opportunistic exploitation targeting known vulnerabilities and widely deployed technologies. The distribution is concentrated, with a small number of attack types accounting for the majority of observed events. Generic path traversal attempts dominate at 28%, indicating large-scale automated probing for directory traversal weaknesses. Andromeda botnet traffic follows at 22%, highlighting sustained botnet-driven reconnaissance and

exploitation activity. HTTP URI SQL injection attempts account for 19%, reflecting persistent efforts to exploit input validation flaws. Additionally, web server password and file access attacks (12%) point to ongoing brute-force and unauthorized access attempts. Lower-frequency but still relevant activity includes Apache Log4j RCE (5%), demonstrating continued exploitation of well-known vulnerabilities. Targeted attacks against common platforms are evident in WordPress path traversal, Phorpiex botnet activity, and PHPUnit eval RCE (each ~3%). More specialized techniques such as remote command shell execution (2%) and Apache CGI path traversal (2%) round out the threat landscape. Overall, the data reflects a blend of high-volume automated scanning and botnet activity, combined with persistent exploitation attempts against widely known and unpatched vulnerabilities.

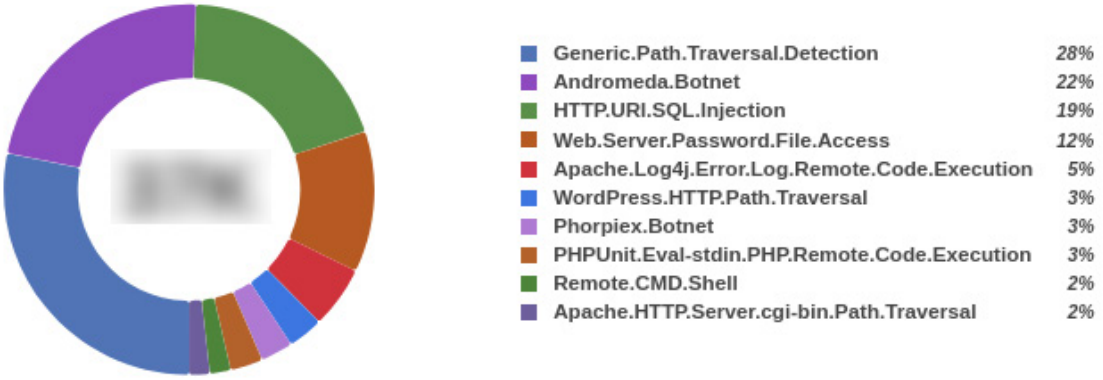


Figure 3. Top IPS Attacks 2025

Web Threat Landscape

The 2025 web attack profile is dominated by information disclosure attempts, which account for 40% of all observed activity—indicating a strong focus on data exposure and misconfiguration probing. Known exploit signatures represent 20%, suggesting continued reliance on publicly documented vulnerabilities. More advanced or systematic probing is reflected in extended generic attacks (15%), while redundant HTTP header manipulation (7%) and generic attacks (4%) show ongoing automated scanning behavior. Lower-frequency but notable categories include HTTP parsing errors (4%), boolean-based injection attempts (3%), and malformed URL/illegal character usage (3%), pointing to fuzzing and injection testing techniques. Minor contributions from crawler activity (2%) and HTTP/2 protocol errors (2%) indicate background scanning and protocol-level probing. Overall, the distribution highlights a mix of opportunistic scanning, exploitation of known weaknesses, and targeted attempts to extract sensitive information.

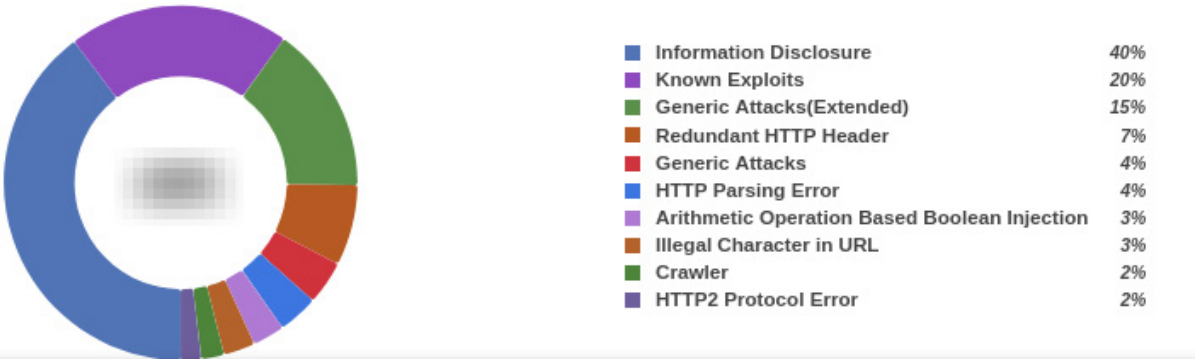


Figure 4. 2025 Top Web Attacks

Lebanon-Specific Threat Landscape (2025)
Lebanon experienced an alarming escalation in cyber threats affecting individuals, government institutions, and critical infrastructure.

Malicious Links and Social Engineering Attacks: Our team analyzed over 100 malicious URLs used to deceive Lebanese citizens. These links were shared through messaging platforms, emails, and social media. Most malicious links impersonated humanitarian organizations offering economic assistance, government ministries claiming to provide support programs, or technical profiles communicating with victims to provide help. These campaigns were designed to harvest sensitive information such as identity documents, phone numbers, locations, and contacts. Several links led to spyware installations capable of silently monitoring victims' devices. Tens of social media accounts (Facebook, Instagram, WhatsApp) were hijacked via phishing pages, and stolen accounts were used to distribute more phishing content or scam messages.

Website Defacements and Government Data Breaches: At least two Lebanese government websites were defaced by attackers who left political or ideological messages. Confidential data from government-related databases was leaked and widely distributed through Telegram, Discord, Reddit, and other forums.

Mobile Threats: At least dozens of malicious Android apps targeting Lebanese users were discovered. These applications were designed to steal private information and gain unauthorized access to device data. The apps requested extensive permissions to access contact lists, SMS messages, GPS location, phone calls, and storage. Distribution methods included third-party app stores, direct messages via Meta, WhatsApp, Telegram, or SMS, and malicious advertisements embedded in popular websites and fake news portals.

Notable Cyber Incident – Ministry Attack: A cyberattack targeted one of the ministries in Lebanon, impacting its primary web application and disrupting normal operations. Following a detailed investigation, it was revealed that the attacker successfully performed lateral movement within the network, leading to the compromise of multiple assets across the environment. Furthermore, intelligence gathered from dark web monitoring confirmed that approximately 6 GB of sensitive data had been exfiltrated and leaked.

Vulnerability assessment Findings: In 2025, the SOC conducted four vulnerability scans. 105 findings from these scans were distributed according to the categories below

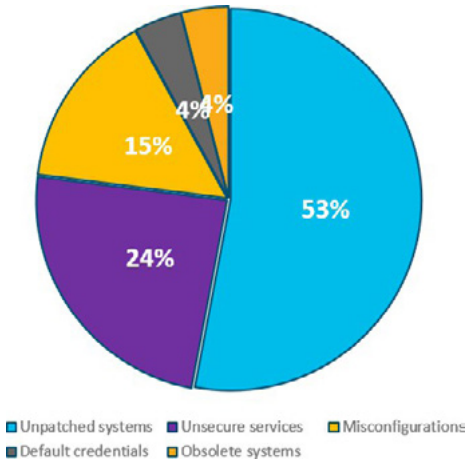


Figure 5. Identified vulnerabilities by category

DDoS Attacks: The SOC detected numerous Distributed Denial-of-Service (DDoS) attacks targeting various network segments. Many of these attacks involved high-bandwidth Fast Floods and Amplification techniques such as DNS, NTP, and SYN floods.

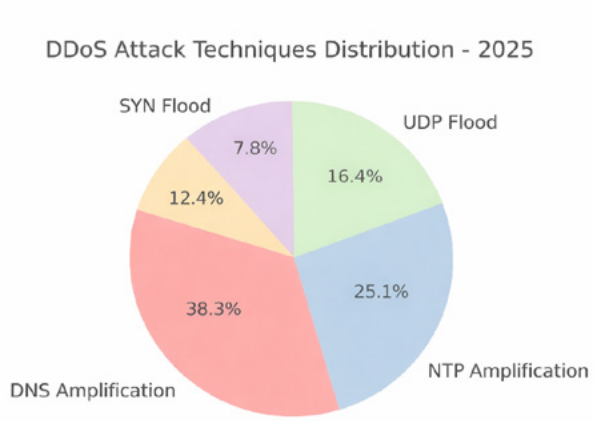


Figure 6. DDoS Attacks Distributions Attacks

Publication(s)

No formal publications were issued during the reporting period. Threat intelligence findings and incident summaries were shared internally with relevant stakeholders and partner organizations.

New service(s)

Enhanced SOC service delivery through:

- New/expanded integrations and log onboarding to increase monitoring coverage.
- Use-case creation and fine-tuning to improve detection fidelity and reduce false positives.
- Quarterly vulnerability assessments to identify and prioritize remediation of weaknesses.
- SOC training for employees/users and threat hunting exercises to strengthen operational readiness and proactive detection.
- Posture Check-up and Post incident Check –up Tables have been prepared to help institution in self-assessment.

In 2025 four general vulnerability scan were conducted, 105 of these scans were distributed according to categories below:

EVENTS ORGANIZED & INVOLVEMENT

Capacity building and stakeholder engagement remained central to the division's mandate in 2025. This section summarizes internal training sessions, threat hunting exercises, awareness campaigns for diverse audiences, and external participation in webinars and job fairs. These events strengthened operational readiness and promoted cybersecurity awareness across Lebanon.

Events organized by the organization / agency

Organized capacity-building activities to strengthen operational security readiness and improve day-to-day SOC effectiveness.

Key activities included:

- **SOC Training for Employees:** A structured training session focused on SOC fundamentals, security monitoring workflows, alert triage, escalation procedures, and incident handling best practices. The training aimed at aligning operational teams on processes, roles, and response expectations.
- **Threat Hunting Exercises:** Practical exercises designed to enhance proactive detection capabilities by guiding participants through hypothesis-driven hunting, log analysis, investigation techniques, and documentation of findings. These exercises supported continuous improvement of detection use cases and operational playbooks.
- **Awareness sessions for internal officers:** Focusing on enhancing understanding of cybersecurity threats, operational security practices, and incident response readiness, tailored to their roles and responsibilities.
- **Awareness sessions for students in universities and schools per age group:** Promoting cybersecurity awareness from an early stage, covering safe internet usage, cyber hygiene, common attack vectors (phishing, malware), and responsible digital behavior.
- **Advanced awareness sessions for Intelligence Bureau officers:** Addressing sophisticated threat landscapes, including cyber threat intelligence, advanced persistent threats (APTs), digital forensics fundamentals, and secure handling of sensitive information.

Events involvement

Actively engaged with the local cybersecurity ecosystem in Lebanon through participation in security-focused webinars and student job fairs. These activities supported knowledge sharing, awareness raising, and talent development by promoting cybersecurity best practices, discussing current trends at a high level, and connecting with students and early-career professionals interested in SOC and cybersecurity roles.

- Participation of the LEBCSIRT team in Cyber Drill, where Lebanon participated thanks to ITU support and Lebanon was ranked Second over 130 Participants even without having the necessary means;
- Participation with Interpol and ITU Table TOP exercises in Qatar
- Participation of the National Cyber Security Coordinator in the ITU _ Study Group -17 on Security Standard representing Lebanon – in December 2025 during which the Arab ST-17 has been created and Lebanon is an active member .\
- Participation in SHANGHAI 2025 where LEBCIRT presented a future analysis and Challenges on Ransomware.
- Participation in multiple workshop

- Organization at the National Level for Civil Servant a Cyber Cybersecurity BOOTCAMP : "Empowerment IT Experts and Leaders on NIS2 Risk and Vulnerability Management.- Mitigate Cyber Risks aligned with EU Standards.
- MCW25 Barcelona where Lebanon presented the LEBCSIRT study about "Mitigating the Future of AI and Cybersecurity"

2026 PLANNED ACTIVITIES

Building on the operational foundation established in 2025, Lebanon's priorities for 2026 focus on advancing national cybersecurity capabilities through a structured and integrated approach combining technical enhancement, operational maturity, capacity development, research and innovation, and strengthened collaboration. These efforts aim to progressively reinforce national cyber resilience while ensuring alignment with international best practices and national priorities.

Detection, Monitoring, and Protection Enhancement
Lebanon will continue to strengthen its national detection and monitoring capabilities through the expansion of SIEM and EDR coverage across critical systems and environments. This includes the integration of additional security-relevant data sources, improved asset visibility, and the progressive extension of endpoint protection and file integrity monitoring mechanisms to critical infrastructure.

In parallel, preventive and access control measures will be reinforced through the introduction of web application protection, network access control, and privileged access monitoring. Proactive threat detection will also be enhanced through the deployment of advanced techniques, including deception technologies, alongside improvements in threat intelligence utilization and threat hunting practices. Continuous advancements in vulnerability management and the automation of threat intelligence ingestion and correlation will further contribute to strengthening the overall security posture.

Incident Response and Operational Readiness
Operational capabilities will be further developed through the refinement of incident response playbooks and standard operating procedures, ensuring a structured and coordinated response to cyber incidents. Regular cyber drills and simulation exercises will be conducted to test readiness, improve coordination, and validate response mechanisms under realistic conditions.

Capacity Building and Awareness
Human capacity development remains a central pillar of Lebanon's cybersecurity strategy. Planned efforts include advanced technical training for SOC analysts and incident responders, the implementation of certification-oriented programs, and active participation in cybersecurity exercises and competitions.

In parallel, awareness and outreach initiatives will be expanded to target public sector entities, educational institutions, and internal stakeholders. These efforts will be supported by the development of multilingual awareness materials and practical guidance aimed at promoting a culture of cybersecurity across sectors.

Research, Innovation, and Advanced Capabilities

Lebanon is placing increasing emphasis on research and innovation as a strategic driver for sustainable cybersecurity development. In close collaboration with the Lebanese University, ongoing initiatives actively engage Master's and PhD students in applied cybersecurity research, contributing to the development of national expertise and a sustainable knowledge ecosystem.

Key focus areas include the exploration of AI-driven cybersecurity solutions to enhance detection, response, and predictive capabilities, as well as the integration of OSINT techniques into investigative and analytical workflows. Research efforts are also being advanced in critical domains such as digital forensics, malware analysis, and cyber threat intelligence, in addition to emerging areas including quantum-related security considerations. This academia–operations synergy supports innovation while ensuring a continuous pipeline of highly skilled professionals.

Collaboration and Strategic Partnerships

Lebanon will continue to strengthen national, regional, and international collaboration through enhanced cooperation mechanisms, participation in joint cybersecurity exercises, and the promotion of structured information sharing across sectors.

Strategic partnerships play a key enabling role in this effort. The continued support of the International Telecommunication Union (ITU), particularly through its regional office in Egypt, contributes to advancing specialized capacity-building programs and technical expertise. Lebanon also aligns with the initiatives of the Arab Council of Ministers of Communications and Information, notably regarding the development of the Arab Threat Intelligence Platform and the provision of tailored support to member states facing capacity and resource challenges. In addition, collaboration with regional entities such as the Dubai Electronic Security Center and the Qatar National Cyber Security Agency remains strategic for knowledge exchange, operational strengthening, and regional interoperability.

Transition Toward a Formal National CSIRT

All planned activities build on the pragmatic approach already adopted through LebCSIRT, which—despite not yet being formally institutionalized—has been effectively delivering core CSIRT-like services, including incident monitoring and handling, threat detection, coordination, and capacity building. This "build-while-operating" model has enabled the validation of processes in real operational conditions, the development of national expertise, and the establishment of foundational capabilities.

As a result, Lebanon is well-positioned to ensure a rapid and effective transition toward a fully institutionalized national CSIRT, with immediate operational impact upon formal establishment.

CONCLUSION

The 2025 reporting year demonstrated tangible progress in SOC maturity, threat detection, and national cyber incident response capabilities. Despite significant resource constraints and an increasingly complex and hostile cyber threat environment, the Cybersecurity Division successfully ensured continuous operational coverage, strengthened monitoring and detection capabilities, and supported high-impact cybercrime investigations and incident response activities.

Throughout the year, the 24/7 SOC-enabled security services provided sustained monitoring, alert triage, investigation, and coordinated incident response. These operational functions were complemented by periodic vulnerability assessments and continuous enhancements to detection capabilities through expanded log source integrations, refinement of detection use cases, and optimization of correlation rules. Collectively, these efforts contributed to improved visibility, reduced noise in alert volumes, and increased operational efficiency across monitored environments.

In parallel, collaboration and information-sharing mechanisms were strengthened, reinforcing coordination across national stakeholders and supporting a more structured and resilient approach to cybersecurity operations under challenging conditions.

Looking ahead to 2026, priorities will focus on further strengthening national cybersecurity capabilities through the expansion of SIEM and EDR coverage, onboarding of additional critical log sources, and enhancement of asset visibility across environments. This will be complemented by the reinforcement of preventive and access control measures, including the implementation of Privileged Access Management (PAM), Web Application Firewall (WAF), and Network Access Control (NAC) capabilities.

In addition, continued investment in human capacity development, advanced training, and operational maturity will remain a central pillar of the national cybersecurity roadmap, ensuring sustained improvement in preparedness, response effectiveness, and overall cyber resilience.

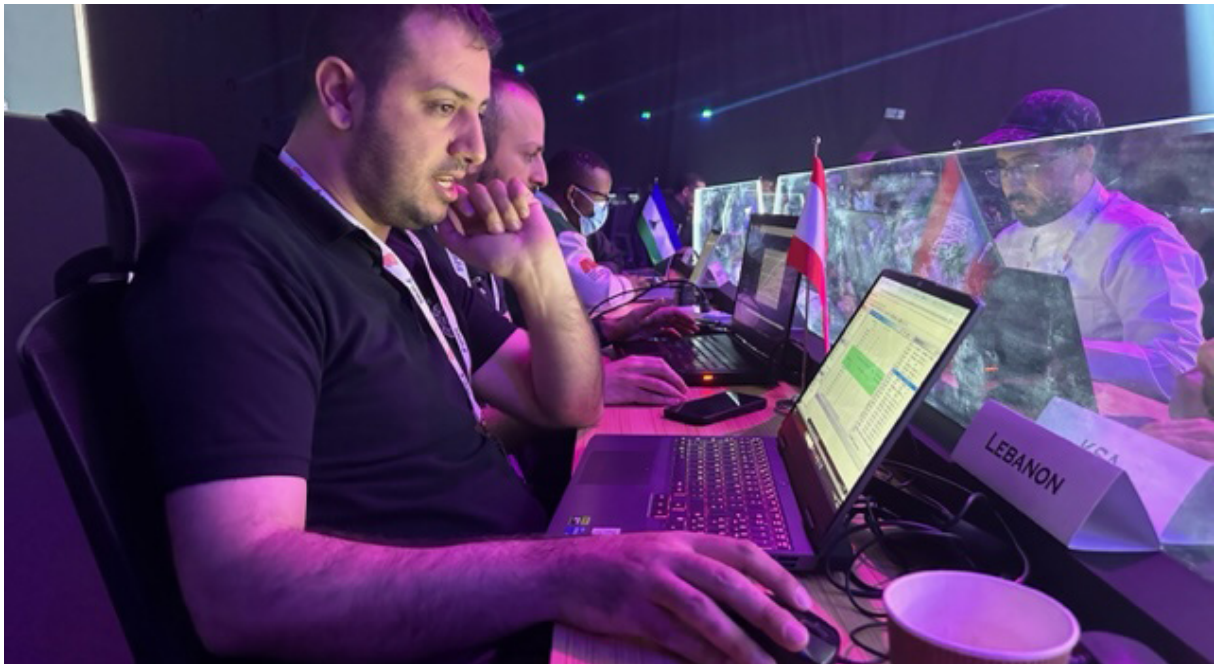
Lebanon also reaffirms its reliance on the continued support of the International Telecommunication Union (ITU), as well as the cooperation of OIC-CERT member states, to further advance national cybersecurity capacity-building efforts and to support the completion of the national CSIRT institutionalization process. This sustained international partnership remains essential to consolidating technical capabilities, accelerating knowledge transfer, and ensuring a timely transition toward a fully operational and formally established national CSIRT.

Contribution of the LebCSIRT Team in MWC25 in Barcelona: Dr. Lina OUEIDAT representing the analysis and research done on the subject with the National Team and the Lebanese University.


MWC25
Navigating the future of AI and Cybersecurity
Dr.Lina OUEIDAT
OIC-CERT Member Leb-CIRT
Lebanon National ICT and Cybersecurity Coodinator


Consolidating Cyber Security Foundation and
HUAWEI

ITUEvents
2025 Global CyberDrill
06-08 May 2025
Dubai, UAE
Lebanon Second Price
over 130 Countries and 260 Participants



CYBERSECURITY BOOTCAMP 1 DECEMBER 2025

SITCEL (Syndicate of Information Technology Certified Experts in Lebanon)

DIGITAL GOVERNANCE &TRUST ACADEMY - BELGIUM


ity Debt in Business activities
Availability risks
Confidentiality risks

STATE OF LIBYA

NATIONAL INFORMATION SECURITY & SAFETY AUTHORITY - NISSA

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

HIGHLIGHTS OF 2025

Summary of Major Activities

In line with the mandate entrusted to the National Information Security and Safety Authority (NISSA), particularly in safeguarding the national critical information infrastructure and enhancing national readiness to respond to cyber incidents and attacks, NISSA continued throughout 2025 to implement its programs and initiatives in accordance with the National Cybersecurity Strategy. These efforts aim to ensure the secure and reliable use of information and communication technologies across both public and private sectors. During 2025, NISSA further strengthened its role as the national umbrella for cybersecurity in Libya by developing regulatory and legislative frameworks, improving compliance with baseline cybersecurity controls, expanding institutional and public awareness, and building national capacities in policies, emerging technologies, electronic authentication, and cyber risk management. The Authority also conducted technical assessments of systems, applications, and digital platforms across governmental and private entities, issuing specialized technical reports, including penetration testing reports, incident reports, and vulnerability assessments. Additionally, NISSA focused on enhancing institutional integration among its departments to operate as a unified and cohesive system, combining regulatory, technical, and awareness aspects, thereby contributing to improving the overall cybersecurity maturity of Libyan institutions.

Achievements

The year 2025 witnessed the implementation of a wide range of activities and achievements, including:

Policy and Regulatory Development:

- Development of the Baseline Cybersecurity Controls document
- Preparation of the Cybersecurity Policy Writing Guidelines
- Update of the Information Security Policy Framework Version 3, including:
  - Identity and Access Management
  - Logging and Monitoring
  - Acceptable Use
  - Endpoint Security
  - Password Management
  - Internet and Email Usage
  - Backup and Recovery
  - Data Classification
- Drafting specialized policies, including:
  - Industrial Systems Security Policy
  - Artificial Intelligence Usage Policy
  - Electronic Authentication and Cryptography Policies

Compliance and Audit Activities:

- Updating the audit checklist to reflect current best practices.
- Adopting a new assessment methodology to accurately measure cybersecurity maturity levels.
- Conducting audits for 27 entities during the period from August to December 2025
- Following up on corrective actions for entities previously audited.

Awareness and Outreach:

- Implementation of national campaigns such as:
  - Safer Summer Campaign.
  - Screen-Free Wednesday Initiative.
- Delivering awareness programs targeting the following sectors:
  - Judicial and Security.
  - Education.
  - Financial and Banking.
  - Telecommunications.

Technical Capacity Development:

- Strengthening technical capabilities in:
  - Industrial Control Systems Security.
  - Artificial Intelligence.
  - Cloud and Virtualization.
  - Public Key Infrastructure (PKI).
  - Internet of Things (IoT).

Human Capacity Building:

- Delivering internal and external training programs.
- Training university students.
- Publishing peer-reviewed scientific papers in accredited journals.

International Engagement:

- Participating in international conferences and events to enhance knowledge exchange.

Adopting an institutional performance measurement system (KPIs) to evaluate and document NISSA projects.

Developing mechanisms for granting cybersecurity service licenses to private sector companies (June 2025).

ABOUT ORGANIZATION

The National Information Security and Safety Authority (NISSA) is the national entity responsible for overseeing information security in Libya and serves as the institutional umbrella under which the Libyan Computer Emergency Response Team (LY-CERT) operates.

The Authority plays a central role in:

- Protecting national critical information infrastructure
- Strengthening trust in ICT usage
- Supporting secure digital transformation

This is achieved through policy development, compliance audits, awareness programs, and capacity building initiatives.

Establishment:

NISSA was established pursuant to Libyan Cabinet Resolution No. (28) of 2013, issued on January 22, 2013.

Resources:

Employees : 70
Scope : National (public and private sectors)
Website : nissa.gov.ly Facebook: facebook.com/Nissa. Libya

ACTIVITIES & OPERATION

Scope and definitions:

In alignment with the National Cybersecurity Strategy, NISSA implemented integrated initiatives aimed at:

- Organizing the Cyberspace.
- Enhancing Cybersecurity Maturity.
- Strengthening Incident Response Capabilities.
- Improving response Capabilities.

Policies, Standards, and Compliance:

- Developing and updating national cybersecurity policies and standards.
- Conducting audits for compliance certification.
- Conducting internal audits within NISSA.

Audit and Assessment:

- Conducting audits on 27 governmental entities.
- Monitoring the implementation of corrective actions.
- Holding coordination meetings with relevant entities.
- Institutional Impact:
  - Enhancing accountability.
  - Establishing a national database for cybersecurity maturity levels.

Awareness and Capacity Building

- Multi-sectoral awareness programs.
- National awareness campaigns.
- Training university and college students
- Participating in conferences and professional events

Key Initiatives:

- Awareness lecture for parents (Safe Digital Environment for Children).
- Participation in Ramadan events discussing cyber extortion.
- Workshops on cyberbullying and phishing.
- Launch of a cybersecurity awareness competition.

Technical Activities

- Development of policies:
  - AI Security
  - IoT
  - Cloud Computing
- Launching of a platform:
  - NISSA AI Platform.
- Developing Security Operations Centre (SOC) operations include:
  - T-Pot threat detection.
  - MISP platform
  - GLPI ticketing system
  - Malware reporting via Team Cymru
  - SIEM (ELK + Wazuh + Cisco Firepower)
- Digital Forensics Laboratory 2025 Activities:
  - Analysis of cryptocurrency mining devices.
  - Log analysis.

EVENTS ORGANIZED & INVOLVEMENT

Key Events

- Cybersecurity Forum (with Libyan Technology Foundation LTF)
- Workshops on:
  - Cyber extortion
  - Cyberbullying
  - Social engineering
- National campaigns:
  - Safer Summer (38 activities)
  - Screen-Free Wednesday.
- Cybersecurity Awareness Month (October 2025).
- Special Sectoral Programs:
  - Judicial and Security Sector.
  - Financial Sector.
  - Educational Sector.
  - Telecommunications Sector.

Events involvement

- International Participation
  - MENA Cybercrime Working Group Doha.
  - Maghreb Cybersecurity Competition Tunisia
  - Regional Cybersecurity Week Morocco
  - The second meeting of Arab Cybersecurity Ministers Council Saudi Arabia
  - Global CyberDrill Dubai
  - INTERPOL training Qatar

Achievements in 2025

- Updating the Baseline of Cybersecurity Controls.
- Auditing infrastructure of 27 governmental entities.
- Issuing new cybersecurity policies and guidelines.
- A total of 470 posts were published, achieving approximately 1.9 million views.
  - Incident Handling
  - Fraud cases
  - Identity theft cases
  - Defamation cases
  - 16 Cyber extortion cases
  - All cases were handled in accordance with established procedures

Technology Achievement

NISSA AI Platform:

- Enhancing incident analysis
- Supporting decision-making processes
- Reducing manual effort
- Improving the efficiency of incident response teams

2026 PLANNED ACTIVITIES

- Continuing the development of cybersecurity policies and standards.
- Continuing compliance audit campaigns.
- Following up on corrective measures.
- Expanding cybersecurity awareness programs.
- Organization of the Cybersecurity Forum scheduled for July 2026 (with Libyan Technology Foundation LTF).
- Enhancing NISSA presence in digital transformation.
- Improving incident reporting and handling mechanisms.

CONCLUSION

In 2025, NISSA successfully reinforced Libya's cybersecurity landscape through comprehensive policy development, technical capacity building, awareness campaigns, and international collaboration. NISSA efforts in auditing, incident handling, and digital forensics enhanced national readiness to respond to cyber threats and improved overall cybersecurity maturity across public and private sectors. Looking ahead to 2026, NISSA aims to continue strengthening regulatory frameworks, expanding awareness initiatives, enhancing technological capabilities, and fostering collaboration at both national and international levels to ensure a secure and resilient cyber environment for Libya.


الدورة العادية
الثانية
لمجلس وزراء الأمن
السيبراني العـــرب
المملكة العربية السعودية - الرياض
ربيع الآخر 1447هـ - سبتمبر 2025م


الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Aut
لأمن وسلامة المعلومات
الإصدار الثاني 2.0
إنترنت آمن
لك ولأطفالك
شهر أكتوبر .. وعي .. تفاعل .. إنجاز
أنشطة الهيئة
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
www.nissa.gov.ly
nissa.libya


منتدى حوكمة المعلوماتية
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
www.nissa.gov.ly
nissa.libya


Electronic Payment
PayNow
مصرف الصحاري
SAHARA BANK
مسارات
مصرف شمال افريقيا
UMHOURIA BANK
Alhada


مشاركات محلية
معرض النيابة العامة الدولي للكتاب - النسخة الثانية
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority


أنشطة شهر التوعية بالأمن السيبراني
المركز العام للتدريب و تطوير التعليم
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
www.nissa.gov.ly
nissa.libya


تدريب
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
www.nissa.gov.ly
nissa.libya


برامج توعوية
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
www.nissa.gov.ly
nissa.libya


GISEC GLOBAL
GLOBAL
CYBERDRILL


الاجتماع الخامس عشر لمجموعة عمل الشرق الأ
وشمال افريقيا حول الجريمة السيبرانية لرؤساء الوحدات
15th MIDDLE-EAST AND NORTH AFRICA
WORKING GROUP MEETING ON CYBERCRIME FOR HEADS OF UNITS
التدريب السيبراني المتخصص
Specialized Tr ssions
DOHA
ITU
مشاركات خارجية
الاجتماع الخامس عشر لمجموعة عمل الشرق الأوسط و شمال أفريقيا
حول الجريمة السيبرانية
الدوحة 2025
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
www.nissa.gov.ly
nissa.libya


شهر أكتوبر .. وعي .. تفاعل .. إنجاز
أنشطة الهيئة
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
www.nissa.gov.ly
nissa.libya


تدريب


برامج توعوية


Cyber Drill
Activities


NISSA LIBYA


Dark Web Leaks

MALAYSIA

CYBERSECURITY MALAYSIA

HIGHLIGHTS OF 2025

Summary of Major Activities

20 - 24 Jan 2025
Co-organised with UK High Commission and BAE UK on IPCP Training:
1. UK – CyberSecurity Malaysia Cyber Cooperation - Review and Further Develop Knowledge and Skills Development (20-22 Jan 2025, 22 participants)
2. Digital Trust Managers (23 & 24 January 2025, 21 participants)

5 Mar 2025
Organised the Webinar through the OIC-CERT Platform "Quantum Computing Threats to the Digital World"

10 Mar 2025
Participated in the APCERT Steering Committee Face to Face meeting, Seoul, South Korea

28 – 30 Apr 2025
Participated in the OIC-CERT Face to Face meeting and the "Future of Digital Countries (FDC) Summit 2025", Cairo, Egypt

8 May 2025
Co-organised sectoral-level Cyber Drill Exercise for Malaysia Capital Markets, participated by 119 organisations, in close partnership with Malaysia Securities Commission (SC) and National Cyber Security Agency of Malaysia (NACSA)

20 – 23 May 2025
Participated in Cyber Games Kuala Lumpur 2025 and scored 4th place (individual) by CyberSEE, CyberEast+, CyberSouth+, GLACY-e and Octopus Projects, in close partnership with INTERPOL and National Cyber Security Agency of Malaysia (NACSA)

26 May 2025
Participated in International Cybersecurity Championship 2025 by Solar RU Group in Cooperation with the Ministry of Digital Development, Communications and Mass Media of The Russian Federation

18 Jun 2025
Organised the ASEAN Webinar "Building Trust in Southeast Asia's Digital Future" in cooperation with Cyber Security Brunei, National Cyber and Crypto Polytechnic Indonesia and Cyber Security Agency of Singapore (online)

18 – 20 June 2025
Two teams participated in Standoff Cyberbattle for SPIEF 2025 by Positive Technologies – First team defending Aviation and Logistics Sector scored 4th place from 12 teams (12 countries), and another team defending Oil & Gas Sector scored 6th place from 13 teams (12 countries)

27 Jul – 10 Aug
Participated in Positive Hack Camp by Positive Technologies, and scored 1st in the final leaderboard and awarded with CyberED Certified Offensive Security Explorer and White Hacker certifications

29 Jul 2025
Exercise Controller (EXCON) for the APCERT Cyber Drill "When Ransomware Meets Generative AI" (online)

19 – 27 Aug 2025
Organised capacity building training under the Malaysian Technical Cooperation Program (MTCP), attended by selected APCERT members, titled "Digital Security & Lifelong Learning Programme" (DLSP)

15 – 19 Sep 2025
Participated in the OIC-CERT Board Meeting and 17th OIC-CERT Annual Conference in conjunction with the Arab Regional Cybersecurity Summit and FIRST & ITU-ARCC Regional Symposium 2025, Rabat, Morocco

30 Sep – 2 Oct 2025
Organised the Cyber Digital Services, Defence and Security Asia (CyberDSA) 2025

1 Oct 2025
Co-Organised ASEAN Programme during CyberDSA "Quantum Safe Migration: Securing ASEAN's Digital Future."

6 – 8 Oct 2025
Participated in Standoff 16 Cyberbattle as Red Team by Positive Technologies

13 – 16 Oct 2025
Co-organised with UK High Commission and BAE UK on IPCP Training - Threat Hunting Training

27 – 31 Oct 2025
Co-organised with UK High Commission and TAG International Team on IPCP Training - Cyber Security Standards and Governance, Risk & Compliance

6 Nov 2025
Participated in AfricaCERT Drill

25 - 27 Nov 2025
Participated in the APCERT Annual General Meeting and Conference 2025, Sydney, Australia
Co organised as Exercise Controller (EXCON) for APCERT Tabletop Exercise (TTX) themed "Responding to Ransomware Using Generative AI"

28 Nov – 1 Dec 2025
Trainer for Artefacts Development Essential for Red Team Operators at Malaysia Cybersecurity Camp 2025

ABOUT ORGANIZATION

Introduction

CyberSecurity Malaysia is the national cybersecurity specialist agency under the purview of the Ministry of Digital Malaysia, having the vision of being a globally recognised National Cyber Security and Specialist Centre. The services provided can be categorised as follows

i. Cybersecurity Responsive Services
   - Security Incident Handling
   - Digital Forensics

ii. Cybersecurity Proactive Services
   - Security Assurance
   - Information Security Certification Body

iii. Capacity Building and Outreach
   - Info Security Professional Development
   - Outreach

iv. Strategic Studies and Engagement
   - Government and International Engagement
   - Strategic Research

v. Industry and Research Development

vi. Cybersecurity Pre-emptive Services

Establishment

CyberSecurity Malaysia started with the formation of the Malaysian Computer Emergency Response Team (MyCERT) on 13 Jan 1997 under the Ministry of Science, Technology, and Innovation Malaysia. In 2023, with the restructuring of the government administration, CyberSecurity Malaysia was put under the purview of the Ministry of Digital Malaysia. CyberSecurity Malaysia is committed to providing a broad range of cybersecurity innovation-led services, programmes, and initiatives to help reduce the vulnerability of digital systems and, at the same time, strengthen Malaysia's self-reliance in cyberspace.

Resources

Cyber Security Incident Response

CyberSecurity Malaysia responds to and handles cyber security incidents through Malaysia Computer Emergency Response Team (MyCERT), Digital Forensics (DF), and Cyber999 Cyber Incident Response Centre (Cyber999). MyCERT and DF departments are the technical reference point for Malaysian organisations facing cybersecurity incidents through on-site services. Cyber999 is a technical reference point for Malaysian Internet users facing cybersecurity incidents through online services. MyCERT, DF, and Cyber999 facilitate the handling and mitigation of cybersecurity incidents for organisations and Malaysian digital users and organisations.

The types of incidents received and responded to are intrusion, fraud, malicious codes, vulnerability reports, intrusion attempts, spam, denial of service (DOS) and data breaches. Cyber999 Cyber Incident Response Centre receives incident reports from various parties in the constituency, such as the general public, the private sector, and SMEs. Additionally, we receive information about incidents involving Malaysian IPs or domains from trusted security teams from abroad (foreign CERTs) and Special Interest Groups such as Shadowserver Foundation and through CyberSecurity Malaysia's proactive monitoring. Cyber999 works closely with ISPs, CERTs, Special Interest Groups (SIGs) and Law Enforcement Agencies (LEAs), from local and international, to remediate and mitigate computer security incidents affecting Malaysia's organisations and the public.

Cyber999 allows Internet users, organisations, and SMEs in Malaysia to report cyber security incidents that threaten Internet users' or organisations' security, safety, and privacy. A list of channels for reporting cyber security incidents to Cyber999 Cyber Incident Response Centre and for getting technical assistance is available at: https://www.mycert.org.my/portal/

Cyber999 responded to 7,616 incidents in 2025, with most reported incidents being fraud, data breach, malicious code, and intrusion.

Constituency

MyCERT and DF constituencies are Malaysian organisations and government agencies that may voluntarily request service related to cybersecurity incidents.

Cyber999 constituencies are non-NCII sectors that include SMEs, businesses and Malaysian Internet users. Cyber security incidents reported to the Cyber999 Cyber Incident Response Centre will be handled and resolved according to the Standard Operating Procedure and Service Level Agreement, together with technical assistance and guidance.

ACTIVITIES & OPERATION

Scope and Definitions

Monthly Cyber Incidents Statistics

Cyber999 proactively produced 200 advisories and 3 alerts in 2025 to inform and warn the constituency about recent cyber threats. The security advisories, alerts, and summary reports produced by Cyber999 Cyber Incident Response Centre can be viewed at https://www.mycert.org.my/portal/advisories2025

Figure 1 shows the reported incidents handled by Cyber999 Cyber Incident Response Centre of CyberSecurity Malaysia.

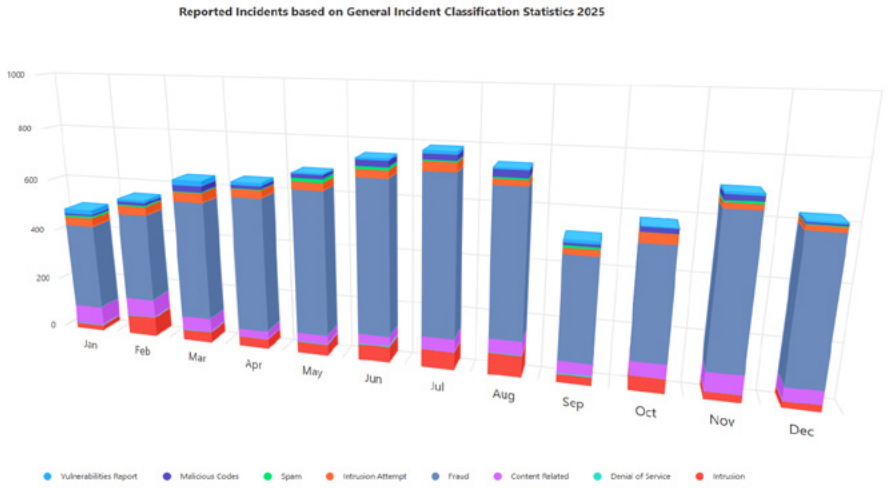


Figure 1: Incidents Reported to Cyber999 of CyberSecurity Malaysia in 2025

The monthly cyber incident statistics can be viewed at: https://www.mycert.org.my/portal/

Security Alert and Advisory

In addition to assisting in technical support for incident handling, Cyber999 also produces security alerts and advisories on the latest cyber threats targeting Malaysia, with reference to patches for software vulnerabilities.

Alerts are urgent notifications about active security threats, vulnerabilities, or ongoing cyberattacks that typically are issued when immediate action is required to mitigate a threat. Cyber999 will provide specific details about the threat issues, affected systems and recommended actions for users to mitigate the threat. While in advisories, Cyber999 will provide information about potential security risks, vulnerabilities, or best practices. Advisories are less urgent than alerts but are still important for long-term security planning for mitigation strategies, patches, and general security recommendations.

A list of Security Alert and Advisory published can be referred to here: https://www.mycert.org.my/portal/advisories

Cyber Incident Quarterly Summary

The Cyber Incident Quarterly Summary Report 2025 provides an overview of computer security incidents handled by the Cyber999 Incident Response Centre of CyberSecurity Malaysia quarterly. Cyber Incident Report also highlights statistics of incidents dealt with by the Cyber999 Incident Response Centre in each quarter of 2025 according to their categories, security alerts and advisories released, and current security threats and trends. It should be noted that the statistics provided in this report reflect only the total number of incidents reported and handled by the Cyber999 Incident Response Centre, excluding elements such as monetary value or aftermaths of the incidents. Computer security incidents dealt with by the Cyber999 Incident Response Centre involved IP addresses and domains from Malaysia.

CyberSOC (Security Operation Centre)

CyberSOC is a centralised facility that integrates various cybersecurity functions and capabilities to enhance an organisation's ability to protect, detect, analyse, and respond to cyber threats more proactively and effectively. It helps to strengthen cybersecurity infrastructure, promote resilience, and protect against both internal and external cyber threats.

This facility managed 3 core services as follows:

- Manage, Detect and Respond (MDR)
- Compromised Network Assessment (CMERP)
- Compromised Endpoint Assessment (EDR/XDR)

The LebahNET Project

LebahNET is a Honeypot Distributed System where a collection of honeypots is used to study the exploits that function as well as to collect malware binaries. Honeypots are computer software mechanisms set up to mimic a legitimate site to ensnare malicious software into believing that it is a legitimate site which is in a weak position for attacks. Honeypot allows researchers to detect, monitor, and counter malicious activities by understanding the activities done during the intrusion phase and attacks' payload. It can be viewed at https://dashboard.honeynet.org.my/

Mobile Assessment Security Scanning Application (MASSA)

MASSA or Mobile Assessment Security Scanning Application is a security tool developed and managed by MyCERT that provides partially automated security scanning for analysts and end-users. This application provides comprehensive information according to the scanning result, enabling analysts to detect any risk or misconfigured security control in an Android smartphone. It identifies any possible entry point for malicious activity, indicator of compromise or possible malicious applications installed in the device. Figure 2 below shows the total devices and applications scanned using MASSA in 2025.

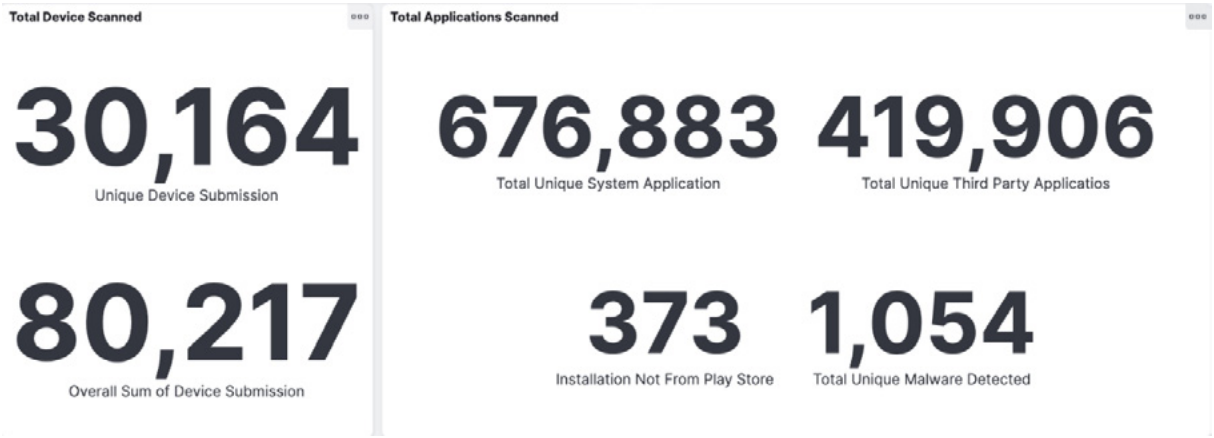


Figure 2: Total Scanned Using MASSA in 2025

Compromise Assessment

MyCERT provides compromise assessment services to help organizations determine whether their systems or networks have been breached. This process involves examining hosts, network traffic, and security logs to identify indicators of compromise, malicious artifacts, and unauthorized activities. By leveraging threat intelligence and forensic analysis techniques, the team can detect potential intrusions and determine their scope and impact, enabling organizations to take timely containment and remediation actions.

Root Cause Analysis

Following a confirmed security incident, Cyber999, MyCERT and DF conduct root cause analysis to identify how the compromise occurred and which vulnerabilities or weaknesses were exploited. By reconstructing the attack timeline and analyzing relevant evidence, the team determines the underlying causes of the incident. The findings support organizations in addressing security gaps, strengthening their defenses, and reducing the risk of similar incidents in the future.

Red Teaming Exercises

CSM also manages and conducts comprehensive red teaming exercises to assess and strengthen security posture of companies and organizations. Through structured adversarial simulations, the team emulates real-world threat actors to identify vulnerabilities across people, processes, and technology. These exercises encompass planning, reconnaissance, exploitation, lateral movement, and reporting, ensuring a realistic evaluation of detection and response capabilities. By delivering detailed findings and actionable recommendations, CyberSecurity Malaysia enables continuous improvement, enhance resilience against evolving cyber threats, and support informed risk management at both operational and strategic levels.

CyberSecurity Malaysia – National AI Office (NAIO) Working Group

CSM actively participates in the National AI Office (NAIO) working group, which aims to develop and implement national action plans to advance the responsible and strategic adoption of artificial intelligence. Through this collaboration, CSM contributes expertise across several key areas, including AI security, AI advisory, AI sovereignty, AI regulation and policy, AI talent development, AI governance and ethics, and AI safety. CSM involvement supports the development of a secure, trustworthy, and sustainable AI ecosystem while ensuring that cybersecurity considerations are integrated into national AI initiatives.

EVENTS ORGANIZED & INVOLVEMENT

Events organized

Malaysian Technical Cooperation Programme (MTCP)
Hands-on training program, titled the Digital Security Lifelong Learning Program (DSLP) under the Malaysian Technical Cooperation Programme (MTCP), was conducted by CyberSecurity Malaysia from 19 – 27 Aug 2025. A total of 13 participants from Commonwealth countries attended the program, representing Bangladesh, Eswatini, Fiji, Gambia, Ghana, Kenya, Lesotho, Malawi, Maldives, Mauritius, Nigeria, Sierra Leone and Sri Lanka.

Indo-Pacific Cyber Programme
CyberSecurity Malaysia together with the British High Commission in Kuala Lumpur and a consortium led by BAE Digital Intelligence (DI) on behalf of the UK Foreign Commonwealth and Development Office (FDCO) had co-organised several capacity-building initiatives under the Indo-Pacific Cyber Programme (IPCP).

These training programmes included :

- UK–CyberSecurity Malaysia Cyber Cooperation training on reviewing and enhancing knowledge and skills development, held from 20 – 22 January 2025 with 22 participants,
- Digital Trust Managers Programme on 23 – 24 January 2025 involving 21 participants.
- Threat Hunting Training from 13 – 16 October 2025 with 11 participants
- Cyber Security Standards and Governance, Risk & Compliance training delivered from 27 – 31 October 2025 with 23 participants.

Drills & exercises
Organised the Capital Market Cyber Simulation (CMCS), a cyber-attack and defence simulation project under the Securities Commission and Cyber Security Malaysia through MyCERT department. CMCS started in 2018 with only 38 participants and has grown rapidly over the years; today, it has 120 participants. For CMCS 2025, the project focuses on simulating real incident scenarios that cover technical assessments and policy adherence through cyber drill platform. This approach ensures seamless accessibility for all participants and enhances their readiness to handle real-world cyber-attack simulations. Additionally, organised cyber drills and Tabletop Exercises (TTX) for the financial sector, supporting the planning, coordination, and execution of cyber incident response simulations to strengthen organisational preparedness and resilience. Also served as Exercise Control (EXCON) for the APCERT Cyber Drill and APCERT Tabletop Exercise (TTX) 2025, contributing to the coordination and execution of regional cyber incident response exercises aimed at enhancing collaboration, information sharing, and collective cyber resilience among APCERT member teams.

Conferences and seminars
Cyber Digital Services, Defence and Security Asia (CyberDSA) is a prestigious annual cybersecurity event held in Kuala Lumpur, Malaysia. The 2025 edition took place from 30 Sep – 2 Oct 2025 at the Malaysian International Trade and Exhibition Centre (MITEC), under the theme "Pioneering the Future: Building a Resilient and Trusted Digital Nation." Organised by CyberSecurity Malaysia, the event is supported by a diverse range of partners from both the public and private sectors, including government agencies, industry leaders, and cybersecurity professionals.

In conjunction with Malaysia's ASEAN Chairmanship in 2025, CyberSecurity Malaysia also identified several ASEAN-related initiatives and events to be implemented throughout the year, further strengthening regional cooperation in cybersecurity and digital resilience.

International partnerships and agreements

The Malaysia Cybersecurity Strategy 2025 identified international cooperation as one of the areas in enhancing cybersecurity. In line with this, CyberSecurity Malaysia is actively establishing collaborative relationships with foreign parties.

Working Visits

CyberSecurity Malaysia conducted working visits to relevant organisations overseas to further enhance the country's cybersecurity posture. The objective of the visits is to seek potential collaborations in cybersecurity. This agency also received working visits from foreign organisations that have similar objectives. Among them are:

i. National Communications Authority (NCA) of Somalia
ii. Brunei Cybersecurity Association (BCSA)
iii. The Russian Trade Mission
iv. Blackfire, Philippines
v. Representatives of the Third Country Training Programme (TCTP) 2025
vi. The Government of Bangladesh (Cabinet Division & Finance Division) and Universiti Putra Malaysia
vii. Cyber Security Brunei
viii. Universiti Teknologi MARA (UiTM) & Standing Committee on Scientific and Technological Cooperation (COMSTECH)
ix. SUE "Cybersecurity centre" ("UZCERT"), Uzbekistan

Events involvement

International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia

i. Asia Pacific Computer Emergency Response Team (APCERT) Steering Committee Member
ii. Member of APCERT Coordinated Vulnerability Disclosure Working Group (CVD WG)
iii. Member of APCERT Policy, Procedures and Governance Working Group (PPGWG)
iv. Member of the Forum of Incident Response and Security Teams (FIRST)
v. Member of the National CSIRT Committee
vi. The Permanent Secretariat of the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT), where a major role is to undertake daily operations and facilitate cooperation and interaction among the member countries
vii. The lead for the Capacity Building Initiatives in the OIC-CERT
viii. Certificate authorising a member of the Common Criteria Recognition Arrangement (CCRA)
ix. Member of the ShadowServer Foundation

x. Member of the ASEAN Forensic Science Network

xi. Member of the Digital Forensics Working Group

xii. Member of the Traffic Accident Reconstruction Working Group

xiii. Member of the INTERPOL Regional Expert Group for Cryptocurrency Investigation (REG-CI)

xiv. Member of the United Nations Office on Drugs and Crime (UNODC) Women in Cyber

xv. Member of the Cybersecurity Alliance for Mutual Progress (CAMP)

xvi. Member of the Women of FIRST SIG

xvii. Member of OWASP Foundation

Cyber Drills & Exercises

CyberSecurity Malaysia participated in two (2) international cyber drills in 2025, namely the APCERT Cyber Drill and the OIC-CERT Cyber Drill.

Seminars & presentations

CyberSecurity Malaysia's representatives had been invited to give presentations and talks at international conferences and seminars as follows:

i. 26 Nov 2025 – Speaker entitled "Helping Analysts Overcome Alert Fatigue Using AI Agent" at the APCERT Annual General Meeting and Conference 2025, Sydney, Australia

ii. 28 – 29 Oct 2025 - As a speaker at the conference entitled "AI for Next-Gen Cyber Threat Detection" at the 46th Edition of The World AI Show

iii. 8 – 9 Oct 2025 - As a speaker at the conference entitled "Securing the Cyber Supply Chain in an Increasingly Connected World" at Cyber Security World Asia (in conjunction with Tech Week Singapore)

iv. 1 Oct 2025 – Speaker entitled "PC Gaming Ubuntu" at Ubuntu Malaysia MiniCon 2025 at CyberDSA, MITEC, Kuala Lumpur

v. 30 Sept 2025 – Speaker and demonstration entitled "Mobile Adversary and Safety Awareness" at CyberDSA, MITEC, Kuala Lumpur

vi. 23 – 24 Sept 2025 - As a speaker at the conference entitled "Challenges of Cybersecurity in Malaysia" at Digital Nation Summit, Kuala Lumpur, ASEAN Edition

vii. 16 -17 September 2025 - As a speaker at the conference entitled "Validating a Set of Candidate Criteria for Evaluating Software Tools and Data Sources for National CSIRTs' Cyber Incident Responses" at the 14th International Conference on IT Security Incident Management and IT Forensics

viii. 21 Aug 2025 – Speaker for Malaysian Ministry of Digital: Digital Talk Series 5: Cybersecurity Trends: May The Resilience Be With You

ix. 21 Aug 2025 – Speaker for ISC2 Malaysia Chapter "Navigating Cybersecurity Certifications For Career Growth"

x. 20 – 21 Aug 2025 - As a speaker at the conference entitled "Digital landscape: Preparing for the next frontier in cybersecurity" at Cybersecurity, IT Assurance, and Governance (CIAG) Conference 2025

xi. 12 – 13 Aug 2025 - As a speaker at the conference entitled "AI-Powered CyberSecurity: Defending Organisations in the Age of Intelligent Threats" at ASEAN AI Summit 2025

xii. 5 – 6 Aug 2025 - As a speaker at the conference entitled "Digital Transformation & Cyber Resilience" at IERP® Global Conference 2025

xiii. 6 Aug 2025 - As a speaker at the conference entitled "Cloud, AI, and Cybersecurity Convergence – Building Resilient Digital Infrastructure" at CloudTech & DataCentre Conference 2.0

xiv. 24 Jul 2025 - As a speaker at the conference entitled "Emerging Threats in the Cyber Landscape: What Malaysian Organisations Need to Know" at Cybersecurity Summit 2025

xv. 21 – 22 Jul 2025 - As a speaker at the conference entitled "Cybersecurity's Role in Crisis Management: Supporting Resilience and Sustainability During Digital Disruptions" at DRI ASEAN 2025 Conference & Award of Excellence 2025

xvi. 15 – 17 Jul 2025 - As a speaker at the conference entitled "Cybersecurity Begins At Home" at ASEAN 5G & OT Security Summit

xvii. 9 – 10 Jul 2025 - As a speaker at the conference entitled "Securing Malaysia's Digital Future: Unifying Efforts in the Age of AI and Emerging Threats" at the 49th Edition of AIBP Conference & Exhibition 2025

xviii. 1 Jul 2025 - As a speaker at the conference entitled "Cyber security in Aviation: Strengthening Airspace Resilience Through Experience and Collaboration" at Cyber Defence & Security Exhibition and Conference (CYDES)

xix. 1 Jul 2025 - As a speaker at the conference entitled "Migration to Quantum-Safe Cryptography: Challenges and Roadmap for Malaysia" at Cyber Defence & Security Exhibition and Conference (CYDES)

xx. 14 -15 May 2025 - As a speaker at the conference entitled "Securing Malaysia's Critical Information Infrastructure: Safeguarding Against Cyberattacks and Data Breaches" at Datacentre & Cloud Infrastructure Summit (DCCI) 2025

xxi. 14 – 16 Jan 2025 – As a speaker at the conference entitled "Threat Analysis on Emerging Data Breach in Malaysia with Causes, Challenges, Preventions, and Moving Forward: at TF-CSIRT Meeting & FIRST Regional Symposium for Europe, Monte Carlo, Monaco

Research Papers

CyberSecurity Malaysia actively contribute research papers to journals and conference proceedings. The following are some of the papers published.

i. A Novel DNA Technique to Strengthen Cryptographic Permutation Tables in Encryption Algorithm - IEEE Access Research Article

ii. Validating a Set of Candidate Criteria for Evaluating Software Tools and Data Sources for National CSIRTs' Cyber Incident Responses - Association for Computing Machinery (ACM)

iii. Conceptual-based Procedure on Data Privacy for Dark Web Data with Standard and Ethical Perspectives – Springer

iv. Enhancement of Privacy Preserving Algorithm Based on K-Anonymization and Homomorphic Encryption on Dark Web Data – Springer

v. A Case Study on Data Privacy Implementation in Higher Education Application Systems in Malaysia - OIC-CERT

vi. A Systematic Literature Review on Continuous Authentication in Zero Trust Architecture for Business - IADITI - International Association for Digital Transformation and Technological Innovation

vii. Investigation And Prosecution Challenges in Financial Crime Investigation: Insights from a Malaysian Survey - OIC-CERT

viii. Study of Cyber Threat Landscape in Malaysia for the Year 2024 - OIC-CERT

ix. Assessment of Third-Party Accessory for Autonomous Driving System in Malaysia - Laboratory of Accident Mechanisms Analysis (LMA) at Gustave Eiffel University, in collaboration with the Society of Automotive Engineers of Japan (JSAE)

x. Toward Quantum-Resilient PKI: A Systematic Literature Review of Post-Quantum Certificates Model - USIM Press

xi. RENTAKA: Detecting Ransomware at Pre-Attack Stage Using Machine Learning Approach – IEEE

Social Media

In 2025, CyberSecurity Malaysia received continuous invitations to speak at cybersecurity events at the local radio and television stations. CyberSecurity Malaysia also actively disseminates cybersecurity concerns through social media such as Facebook, Instagram, Threads and X, which as of now the Facebook Page has about 65,000 followers, the CyberSecurity Malaysia X has 8,104 followers, CyberSecurity Instagram has 10,000 followers, and CyberSecurity Malaysia Threads has 1,849 followers.

2026 PLANNED ACTIVITIES

To encourage a safer cyber environment, CyberSecurity Malaysia realises the need to work together with the local and international cybersecurity organisations through the establishment of formal relationship arrangements, such as through Memorandum of Understanding (MoU) and agreements.

CyberSecurity Malaysia and Aerosea Exhibitions Sdn. Bhd will be organising an international event known as the Cyber Digital Services, Defence and Security Asia (CyberDSA'26). This event is scheduled to take place from 5 to 7 October 2026, at the MITEC, Kuala Lumpur. CyberDSA aspires to be a leading content-driven event, serving key stakeholders protecting national, public and business interests in cyberspace. It aims to connect decision makers in governments and the private sector to accelerate the digital drive with security on a regional scale. This event aims to impart the latest knowledge and insights while showcasing cutting-edge technologies that would safeguard digital economies and foster global competitiveness. At the international arena, CyberSecurity Malaysia, as the Permanent Secretariat of the OIC-CERT, continues to spearhead collaborations and organise international events such as the OIC-CERT Annual Conferences and Trainings. With such understanding, CyberSecurity Malaysia supports newly established local and international CSIRTs by providing consultation and assistance, especially in becoming

members of the international security communities such as the APCERT, FIRST, and OIC-CERT. CyberSecurity Malaysia aims to develop GSOC and GCSIRT capabilities while strengthening local development of cybersecurity technologies, such as SOAR, EDR, and NDR. In addition to conducting cyber drills at the sectoral level, CyberSecurity Malaysia also plans to expand these exercises to the organizational level to further enhance incident preparedness. These initiatives will support the long-term vision of integrating all cybersecurity domains into a unified Digital Fusion Center to enable more coordinated monitoring, analysis, and response capabilities.

CyberSecurity Malaysia strives to improve its service capabilities and encourages local Internet users to report cybersecurity incidents to the Cyber999 Cyber Incident Reference Centre. The development of new and better reporting channels and further promotion of services through the mass media are aspects that will be intensified.

CONCLUSION

CyberSecurity Malaysia will continuously work with international allies to generate useful cooperation in safeguarding the cyber environment. The agency will work together to meet APCERT's vision to create a safe, clean, and reliable cyberspace in the Asia Pacific region.

In line with the CyberSecurity Malaysia Strategy to emphasise capacity and capability building, mitigation of cyber threats, and international collaboration, CyberSecurity Malaysia will continue to enhance existing and develop new cybersecurity processes, capabilities, and technologies. CyberSecurity Malaysia will also continue with the commitment to seek new edges in cybersecurity and to be a catalyst in developing the industry.

International cooperation and collaboration are essential facets in mitigating cybersecurity challenges. Since cyberspace transcends physical national boundaries, strong international relations will remain a critical initiative. With the rapid development of the internet, economies increasingly depend on public network applications such as online banking, online stock trading, e-business, and e-governments, making the protection of national information infrastructures a global priority.

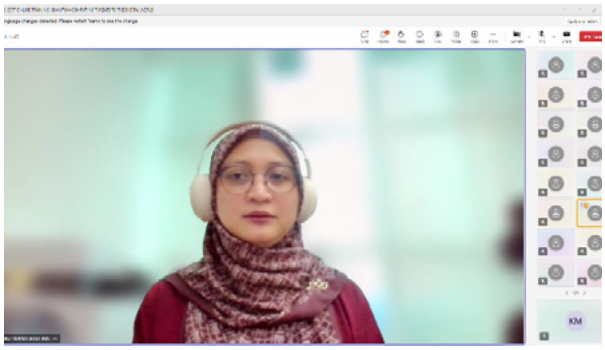
Looking ahead, artificial intelligence (AI) will play a pivotal role in strengthening cybersecurity. AI-driven tools can enhance threat detection, automate responses, and predict emerging risks, but they also introduce new vulnerabilities that require coordinated oversight. Therefore, collaboration must extend beyond traditional frameworks to include shared AI governance, ethical standards, and joint innovation in AI-powered defense systems.

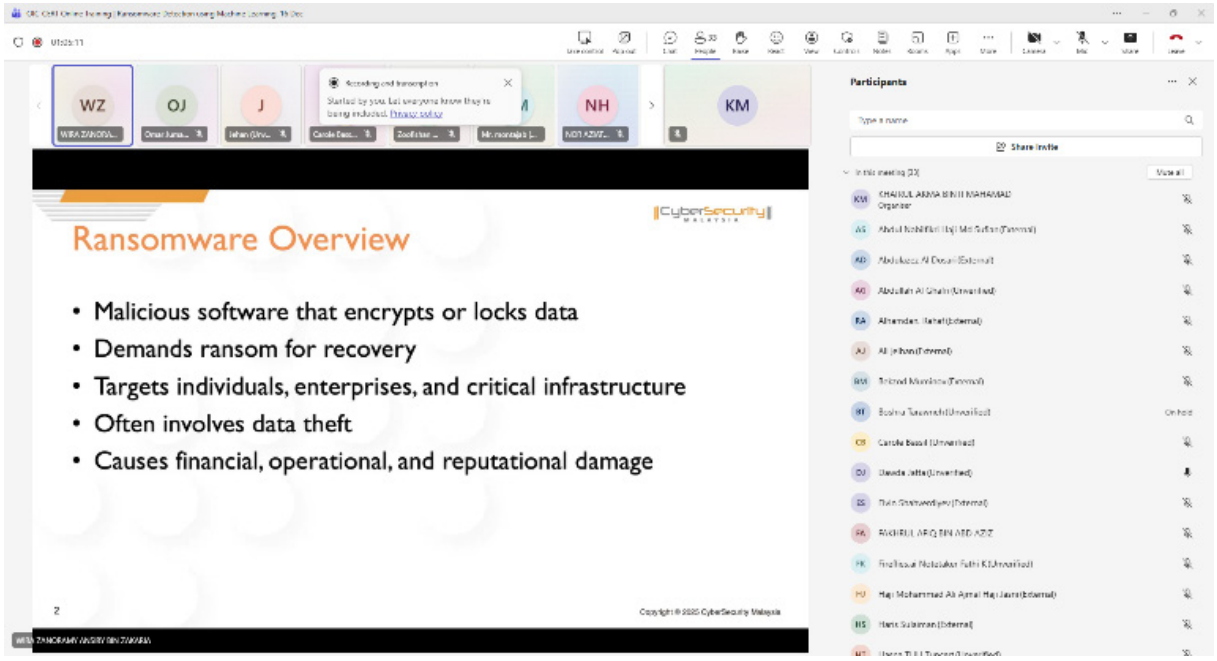
CyberSecurity Malaysia will continue to establish and support cross-border collaboration through bilateral and multilateral platforms, while also pursuing new partnerships with cybersecurity and AI agencies regionally and globally. By combining human expertise with AI capabilities, we aim to make cyberspace a safer, more resilient environment for all.

Photos during event of CyberDSA 2025

MTCP 2025 participants

Online training hosted by CyberSecurity Malaysia

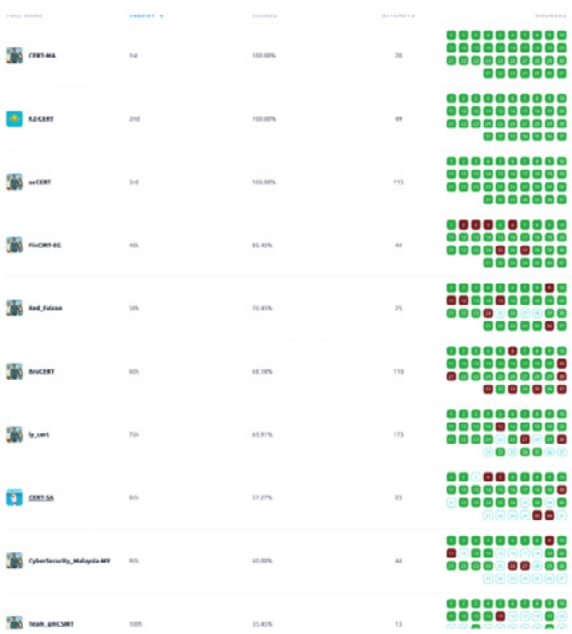




Positive Hack Camp by Positive Technologies, 27 Jul – 10 Aug: Closing ceremony of the camp with shortlisted students across countries. Representative from CyberSecurity Malaysia: Muhammad Fitri Bin Mohd Sultan (MyCERT)

Cyber Games Kuala Lumpur 20- 23 May 2025: CyberSecurity Malaysia's representatives - Fatahillah Bin Hashim (MyCERT), Syafiq Iskandar Bin Sham Suri (Cyber999) and Jayhanraaj A/L Jeeva (Digital Forensics)

OIC-CERT 13th Regional Cyber Drill 17 Sept 2025: CyberSecurity Malaysia scored 9th place



Standoff Cyberbattle SPIEF as Blue Team on 18th – 20th June 2025 by Positive Technologies: First team, Pasukan Biru, defending Aviation and Logistics Sector scored 4th place from 12 teams (12 countries), and another team, Cyber1000, defending Oil & Gas Sector scored 6th place from 13 teams (12 countries).

Ranking of teams defending the logistics industry

Position	Country	Team	Attacks investigated
1		S.H.I.E.L.D	7 of 7
2		CyberTeam	7 of 7
3		beCloud	7 of 7
4		Pasukan Biru	3 of 7

Ranking of teams defending the oil and gas industry

Position	Country	Team	Attacks investigated
1		N@mela$$	7 of 7
2		S-Bastion Lab	7 of 7
3		czon3	7 of 7
4		SAS.PDV	5 of 7
5		Heroes Cyber Security	4 of 7
6		Cyber1000	4 of 7

Participated in Standoff 16 Cyberbattle as Red Team on 6 – 8 Aug by Positive Technologies: Scored 13th place out of 24 teams

MyCERT delivered training on "Artefacts Development and Persistence for Red Team Operators" to UZ-CERT team

Indo-Pacific Cyber Programme (IPCP) Threat Hunting: Endgame on 18 – 20 Nov 2025

Nur Sarah Jamaludin, speaker entitled "Helping Analysts Overcome Alert Fatigue Using AI Agent", and Tabletop Exercise Controller (EXCON) at the APCERT Annual General Meeting and Conference 2025, Sydney, Australia

NIGERIA

CS2-CERT

HIGHLIGHTS OF 2025

Summary of Major Activities

Facilitated Nigeria Data Protection Commission (NDPC) Training and Certification of Data Protection Officer successfully completed. Facilitated Ministry of Foreign Affairs Seminar on Anticipatory, Cyber and Digital Diplomacy for strengthening Nigeria Foreign Policy and Provision of Comprehensive Privacy and Security Audit of National Digital Identity Management Systems (NIMS) Infrastructure and Ecosystem for Nigeria Digital Identification for Development (ID4D) Project successfully completed. Subject-Matter Expert on Emerging Technologies in Security, Conflict and Disarmament for the African Union Disarmament Fellowship (AUDF) Training Manual Development

Achievements

- Completed Nigeria Data Protection Commission Training and Certification of Data Protection Officer.
- Completed Ministry of Foreign Affairs Seminar on Anticipatory, Cyber, and Digital Diplomacy.
- Completed Nigeria Digital Identification for Development Project (ID4D) for a Comprehensive Security and Privacy Audit of National Identity Management System (NIMS) Infrastructure and Ecosystem.

ABOUT ORGANIZATION

Introduction: Consultancy Support Services (CS2) Limited is a cybersecurity and data governance consultancy delivering national security policy, ICT and emerging technology policy, capacity building, and organisational effectiveness services.

Establishment: CS2 was incorporated in Nigeria on 13 February 2002 under the Companies and Allied Matters Act.

Resources: CS2 maintains multidisciplinary capabilities spanning:

- cybersecurity and digital forensics
- information management and systems networking
- ICT infrastructure and programming
- digitisation, archiving, and digital libraries
- change management and enterprise systems

Constituency: CS2 serves public and private sectors, academia, media, and civil society, operating across Nigeria, Africa, and international environments.

Synthesis: CS2 functions as a multidisciplinary policy–technical advisory firm bridging cybersecurity, governance, and institutional capacity across national and continental contexts.

ACTIVITIES & OPERATION

Scope and definitions

Scope: CS2 establishes its operational scope as integrated advisory and professional services across cybersecurity, data governance, and ICT policy domains, covering the design, audit, and strengthening of national and sectoral security architectures; the development of data governance frameworks, compliance tools, and regulatory capacity aligned with national laws and AU instruments; the drafting and implementation of national, regional, and continental digital and cybersecurity strategies; structured capacity building through training, certification, and institutional strengthening for policymakers, regulators, and practitioners; facilitation of multi-stakeholder engagement to secure policy adoption and ownership across government, private sector, and civil society; and advisory support for digital transformation, including identity systems, infrastructure, and governance models underpinning digital economies.

Definitions (Operational Framing): CS2 applies a defined operational lexicon to structure engagements, where cybersecurity denotes the protection of digital systems, networks, and critical information infrastructure against disruption, compromise, and abuse; data governance defines the institutional, legal, and technical frameworks regulating the collection, processing, sharing, and protection of data; digital resilience establishes the capacity of institutions and systems to anticipate, withstand, recover from, and adapt to cyber and digital risks; capacity building requires the structured development of human, institutional, and technical capabilities for effective policy implementation and enforcement; policy and strategy development defines the translation of national and continental mandates into operational frameworks, instruments, and implementation pathways; and multi-stakeholder engagement establishes coordinated participation of public, private, and civil actors to ensure legitimacy and sustainability of governance processes.

Abuse Statistics Extract (INTERPOL Africa Cyberthreat Assessment Report 2025)

Prevalence and Incident Share

- Cybercrime >30% of all crimes in Western and Eastern Africa subregions.
- Over two-thirds of African member states report cyber-dependent/enabled crimes as a medium–high share of total crime.

Financial Abuse and Losses

- > USD 3 billion estimated cybercrime losses across Africa (2019–2025).
- USD 193 million linked to disrupted cybercrime schemes in Operation Serengeti.
- Example BEC case: USD 19.6 million stolen from 400+ victims.

Online Scams and Phishing Abuse

- Phishing accounts for 34% of all cyber incidents in Africa.
- Online scams identified as most prevalent cyberthreat continent-wide.

Sextortion and Online Abuse

- >60% of countries report an increase in digital sextortion incidents.
- 63,000 Instagram accounts and 7,000 Facebook entities removed (Nigeria-linked sextortion networks).
- 250,000+ sextortion-related appeals recorded in Egypt (2024).

Reporting and Enforcement Gap Indicators

- Only ~35% of cybercrimes are officially reported, implying significant undercount of abuse.
- 10,490 cybercrime-related arrests reported across 19 African countries (2024).

Ransomware and Data Abuse Indicators

- Ransom demands range from thousands to millions of USD per incident.
- Example breach: 626.3 GB data leaked; >619,000 individuals affected (Telecom Namibia).

Growth and Abuse Trends (Operational Indicators)

- Scam notifications show extreme increases (e.g., +2,930%, +3,310%) in specific countries (Figure 4, p.13).
- 38% increase in cybercrime-as-a-service (CaaS) targeting business email accounts.

Sub-Region	Cybercrime Share of Total Crimes	Top Threats
West	>30% (High)	Phishing, BEC, Ransomware interpol https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa
East	>30% (High)	Phishing, Ransomware interpol https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa
North	Medium	Online Scams, Sextortion
Central	Medium	BEC, Identity Theft
South	Medium	Ransomware, DDoS

Synthesis:
Abuse in Africa is characterised by scale (≥30% crime share), monetisation (>USD 3bn losses), and underreporting (~65% unseen).
Social engineering abuse vectors (phishing, scams, sextortion) dominate both frequency and victim impact.

Publication(s)

- Artificial Intelligence for Africa's Defence Force Toolkit https://africacenter.org/toolkit/artificial-intelligence-for-africas-defense-force-toolkit/
- Anticipatory, Cyber, Digital, Diplomacy, Master Class Series for African Diplomats https://www.youtube.com/@AnticipatoryCyberDigitalDiplo
- Sovereign by Design: Africa's Data Security Governance Playbook, Advancing Data Sovereignty: Security, Resilience & Trust for Africa's Digital-Intelligence Era - Whitepaper https://iipp.africa/sovereign_by_design.php
- The African Digital Compact. https://au.int/en/documents/20240809/african-digital-compact-adc
- African Lessons in Cyber Strategy (Africa Center for Strategic Studies) https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/
- GCSC-Advancing Cyberstability Final-Report-November-2019 https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf
- Digital Rights in Society of Frontiers of Tech Governance Initiative Inc., and the Paris Peace Forum https://tj4c50.a2cdn1.secureserver.net/wp-content/uploads/2022/03/Initiate-PPF-Global-South-AI-Report-EN.pdf
- Towards Identifying Critical National Infrastructures in the National Cybersecurity Strategy Process https://thegfce.org/tools/towards-identifying-critical-national-infrastructures-in-the-national-cybersecurity-strategy-process/
- Beyond the North-South fork on the AI road – a roadmap towards democratic and distributive integrity https://tj4c50.a2cdn1.secureserver.net/wp-content/uploads/2022/03/Initiate-PPF-Global-South-AI-Report-EN.pdf
- Towards a Global Framework for Cyber Peace and Digital Cooperation: An Agenda for the 2020s - African perspective https://drive.google.com/file/d/1RFEgNU6lMMnaMpP-CRbfzBOzvnIY6Wn1/view
- African Continental Cybersecurity Strategy (ACCS) (2025-2030) [draft]

New service(s)

- Data Protection Impact Assessment (DPIA) is a structured process required under the Nigeria Data Protection Act (NDPA) 2023
- Training of Data Protection Officers

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- Training and Certification of Data Protection Officer for Nigeria Data Protection Commission (NDPC)
- OIC-CERT Cyber Drill 2025.
- Inaugural Seminar on Anticipatory, Cyber and Digital Diplomacy for Strengthening Nigeria's Foreign Policy for Ministry of Foreign Affairs.

Events involvement

- Participated in OWASP SAMM Training Virtual – 16 to 17 January 2025
- Facilitated in Training and Certification of Data Protection Officer, Abuja – 20 to 24 January 2025
- Participated on ADRH Data Protection Assessment (DPIA) Masterclass, Virtual – 04 February 2025
- Participated in Geneva Dialogue Masterclass #6 on ICS Security in Context of CIP, Virtual – 07 February 2025
- Participated in OEWG – UN Framework on Responsible State Behaviour in Cyberspace, New York – 18 February 2025
- Participated in Conference de Presse du Cyber Africa Forum (CAF) 2025, Benin Republic – 26 February 2025
- Participated in Geneva Dialogue Masterclass #7: Responsible Behaviour of Private Actors during Peace and War time, Virtual – 04 March 2025
- Participated in First Open Consultation for Africa IGF, 2025, Virtual – 10 March 2025
- Participated in Responsible Governance of Commercial Cyber Intrusion Capabilities in Africa, Virtual – 11 March 2025
- Participated in the Introduction to the Formulation of Future o a Continental Cybersecurity Project, Virtual – 18 March 2025
- Participated in Huawei-NDPC NADPA Team – Data Security Guidance, Virtual – 03 April 2025
- Participated in Geneva Dialogue Consultation #5, Virtual – 09 April 2025
- Speaker/ Panellist Discussion at GS-CDP Summit 2025, Virtual – 11 April 2025
- Participated in Geneva Dialogue Masterclass #8: Securing Data Across Critical Infrastructure Supply Chains, Virtual – 17 April 2025
- Participated in White Paper on Data Security Governance, Virtual – 22 April 2025
- Participated in Regulatory Approaches to Data Privacy in Africa, Transcorp Hilton, Abuja – 06 May 2025
- Participated in Dutch Ministry of Foreign Affairs – Interview GFCE, Virtual – 09 May 2025
- Participated in Global Conference on Cyber Capacity Building (GC3B), Switzerland – 13 to 14 May 2025
- Participated in West African Internet Governance Forum 2025, Abuja – 20 to 23 May 2025
- Participated in Continental Cybersecurity Strategy Forum on the Ethics of Artificial Intelligence, Virtual – 27 May 2025
- Participated in Introductory meeting: Potential Collaboration on Cybersecurity for South Africa, Virtual - 28 May 2025
- Participated Geneva Dialogue masterclass #10, Virtual – 03 July 2025
- Participated in Africa Endeavor 2025, Benin Republic – 07 to 11 July 2025
- Facilitated Seminar on Anticipatory, Cyber and Digital Diplomacy for Strengthening Nigeria's Foreign Policy, Abuja – 02 to 03 September 2025
- Participated in Panel, Digital Trade: Leveraging Identity for Cross-Border Interoperability for Financial Inclusion, Abuja – 16 September 2025

- Participated in Regional Briefing on Science and Technology Matters for Africa ahead of the 80th Session of the First Committee of the UN General Assembly, Virtual – 17 September 2025
- Participated in 1st Common Good Cyber Fund Strategic Advisory Committee meeting, Virtual - 23 September 2025
- Participated in Cyber Security Program with INSETA, Virtual – 30 September 2025
- Participated in Thematic consultation #8 "Non-tangible harms to critical Infrastructure, Virtual – 09 October 2025
- Participated Nigerians in Diaspora & the New Tax Laws, Virtual – 10 October 2025
- Speaker at AU on Securing Africa's Digital Future: Cybersecurity Challenges and Opportunities, Virtual – 16 October 2025
- Participated in GFCE ACE Enhancement Webinar #3: Cyber Risk is a Team Sport - Third-Party Risk in Financial Institutions, Virtual – 22 October 2025
- Participated in Geneva Dialogue: Masterclass #12, Virtual – 29 October 2025.
- Participated in Advancing Cybersecurity and Cyber Diplomacy in Africa, Virtual – 30 October 2025.
- Participated Coordination call for Workshop 1 in 3rd African Forum Cybercrime, Virtual – 06 November 2025.
- Participated in Africa's Scam Landscape: Insights & Strategies from Key Markets, Virtual – 11 November 2025.
- Participated in Geneva Dialogue: Masterclass #13, Virtual – 13 November 2025.
- Participated in AU Peace and Security in Cyberspace, Marcus Addis Ababa – 18 November 2025
- Participated in The Future of Workforce and How AI & Cybersecurity are Redefining Careers, Virtual – 19 November 2025
- Participated in Geneva Dialogue: Thematic consultation #9 (Cyber Harm, Part 2), Virtual – 20 November 2025
- Participated in Workshop 7 – "Data protection as an enabler for international cooperation on cybercrime", Nairobi, Kenya – 26 November 2025
- Participated in FIRST.Org Symposium Africa & Arab Regions Program Overview Agenda, Mauritius – 02 to 07 December 2025
- Participated in OIC-CERT training session | "Ransomware Detection using Machine Learning", Virtual – 16 December 2025

2026 PLANNED ACTIVITIES

- Continuous involvement in Organisation of Islamic Cooperation-Computer Emergency Response Team (OIC CERT); Global Forum on Cyber Expertise (GFCE); African Union Cybersecurity Expert Group (AUCSEG); Global Commission on the Stability of Cyberspace (GCSC); Internet Corporation for Assigned Names and Numbers (#ICANN), Nigeria Computer Society (NCS); Computer Professionals Registration Council of Nigeria (CPrN); Cyber Security EXPERTS association of Nigeria (CSEAN) and related activities.
- Continuous in-house cyber-forensics capacity development program.
- Give services in support of Military-Civilian, Law Enforcement and related Cybersecurity Initiatives.

- Collaborate with the Government Inter-Agency Committees on the implementation of Cybersecurity measures.
- Support the following national initiatives:
  - Implementation of Nigeria Data Protection Policy.
  - Implementation of a Nigeria Data Protection Roadmap.
  - Harmonisation, standardisation, and seamless interoperability of national identity systems as well as evolving a Business Model/ Plan defining the rules of engagement governing access of Foundation Identity by Agencies/ organisations providing Functional national identity.
  - Strengthening of ICT departments in our Higher Education Institutions (HEIs).
  - Development of a blueprint of common services, policies, standards, procedures, and technical components that guide Ministries Departments and Agencies (MDAs) on IT investment.

CONCLUSION

This report establishes that cybercrime in Africa has transitioned from episodic criminal activity to a persistent, structured, and economically significant threat environment. The evidence confirms scale, monetisation, and systemic underreporting as defining characteristics, with social engineering vectors dominating both frequency and impact.

CS2-CERT's interventions in 2025 demonstrate that capability development, policy alignment, and institutional strengthening can convert national exposure into operational resilience. Targeted actions in data protection, digital identity assurance, and cyber diplomacy have established practical pathways for integrating governance, security, and international cooperation.

However, current response architectures remain constrained by fragmented legal frameworks, limited enforcement capacity, and insufficient cross-border coordination. These constraints directly weaken deterrence and allow transnational cybercrime ecosystems to persist.
The report therefore requires a shift from reactive enforcement to structured cyber resilience. This requires:

1. institutionalised public–private operational cooperation
2. data-driven regulatory intelligence and incident visibility
3. harmonised legal and policy frameworks aligned with continental and global instruments
4. sustained investment in human capital and technical capability

Cybersecurity now functions as a core pillar of economic stability, digital sovereignty, and national security.

CS2-CERT remains positioned to support OIC-CERT and Member States through technical expertise, policy advisory, and capacity-building interventions that convert strategy into operational capability.

Group Photos of NDPC Official and Participants at the Training

Group Photos of NDPC Official with Participants at the Training

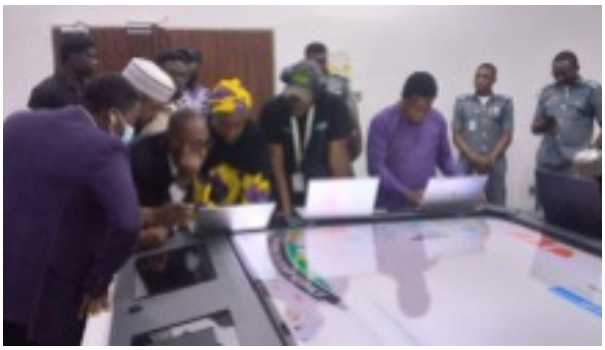
Cross Section of Participants During the Training

Group Photograph of Ministry of Foreign Affairs Officials and Seminar Participants on Anticipatory, Cyber and Digital Diplomacy

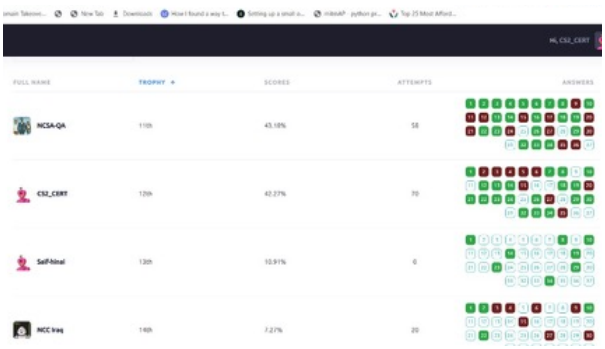
Group 1 Participants brainstorming during the Seminar

Group 2 Participants brainstorming during the Seminar

Group Photograph of Participants at OIC-CERT Cyber Drill 2025

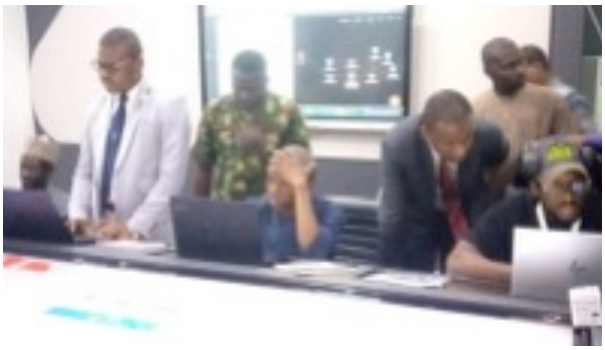


Players and Observers exchanging views on the Injects During the Drill

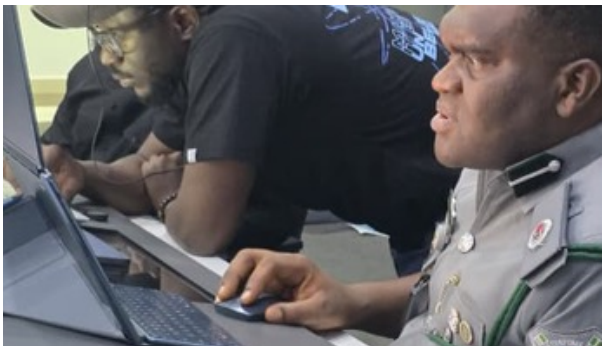


OIC-CERT Cyber Drill 2025 Score Board

Participants in Action during the Cyber Drill



Players exchanging views on the Injects during the Drill



Players Analyzing and Responding to the Drill Injects

PAKISTAN

NCCIA / NR3C

HIGHLIGHTS OF 2025

Achievements

- Muhammad Akram Mughal, Deputy Director (Network Security), NCCIA Pakistan, led the NCCIA team in the "13th Arab Regional, OIC-CERT & Africa Cyber Drill", held on 18 September 2025 in Rabat, Morocco. The drill was organized under the OIC-CERT framework and hosted by Morocco. Under his leadership, the NCCIA team secured 3rd position among cybersecurity teams from 57 Muslim member states, bringing significant recognition to both NCCIA and Pakistan. This achievement reflects his professionalism, dedication, and strong leadership in the field of cybersecurity.
- Muhammad Akram Mughal, Deputy Director (Network Security) at NCCIA Pakistan, earned the Certified Ethical Hacker (CEH) Version 13 (V13) certification on 19 May 2025, achieving an outstanding score of 96.8% in a rigorous four-hour examination.
- NCCIA received total 157,826 cybercrimes/cybersecruity incidents complaints accross Pakistan in the year 2025.
- International Recognition: Secured 3rd position in the 13th OIC-CERT Cyber Drill 2025 among cybersecurity teams of 57 member states, highlighting Pakistan's growing cyber defense capabilities.
- Capacity Building & Training: Conducted multiple awareness sessions and trainings on cyber laws, online safety, and cybercrime complaint mechanisms for national institutions including National Database and Registration Authority and leading universities.
- Academic & Policy Engagement: Delivered expert lectures at premier institutions such as Ghulam Ishaq Khan Institute of Engineering Sciences and Technology and National Defense University Islamabad, contributing to national discourse on cybersecurity, media regulations, and governance.
- International & Development Sector Collaboration: Partnered with organizations like Centre for Peace and Development Initiatives (supported by the European Union) to promote cyber awareness and digital safety.
- Professional Excellence: Officers of NCCIA achieved globally recognized certifications, including CEH v13, enhancing institutional technical expertise.

- Public Awareness & Outreach: Organized seminars, workshops, and briefings to educate diverse stakeholders—including government officials, academia, and civil society—on emerging cyber threats and legal frameworks.
- Case Resolution & Arrests: Investigated 2,196 major cybercrime cases, resulting in 2,902 arrests and 774 successful prosecutions (a 36% resolution rate).
    - **Financial Impact:** Recovered over 461 million PKR in stolen assets and froze 46,056 fraudulent bank accounts and digital wallets.
    - **Dismantling Syndicates:** Disrupted five major organized cybercrime syndicates operating both domestically and internationally.
    - **Major Raids:** * July 2025: A massive raid on a factory in Faisalabad led to the arrest of 149 individuals, including 48 Chinese nationals and several other foreign nationals, dismantling a major organized cyber network.
    - **June 2025:** Arrested suspects in Multan involved in a massive 20 billion PKR online fraud scheme.
    - **Operation Brown:** A specialized initiative launched in late 2025 targeting online child exploitation, which resulted in 35 high-profile arrests.
    - **Public Outreach:** Conducted a campaign reaching roughly 2 million citizens to educate them on phishing, identity theft, and safe digital practices.
    - **24/7 Helpline:** Operationalized the 1799 helpline to provide immediate assistance for cyber harassment and fraud.
    - Under the leadership of Director General Syed Khurram Ali (appointed October 2025), the agency underwent a significant overhaul:
    - **AI & Machine Learning:** Deployed advanced cyber intelligence platforms and trained over 300 officers in their use.
    - **International Cooperation:** In April 2026, the DG announced upcoming MoUs with the US (FBI) and China to streamline cross-border investigations.
    - **Infrastructure Expansion:** Acquired a dedicated three-story HQ building in Islamabad and neared completion of a new regional office in Lahore.
- New Recruitment: Announced the hiring of additional officers to address the manpower shortage and the backlog of complaints.

ABOUT ORGANIZATION

Introduction

- NR3C was established in 2007 as a PSDP funded Project.
- All officers and Man Power of NR3C was regularized in 2012.
- All officers inducted in phase-II and phase-III of NR3C are in process of regularization (permancy).

- Enactment of Prevention of Electronic Crimes Act (PECA), 2016 through Parliament of Pakistan, converted NR3C into Federal Inbestigation Agency (FIA) Cyber Crime Wing (CCW).
- NR3C/FIA CCW was legally mandated to ennforce Prevention of Electronic Crimes Act, 2016. Parliament of Pakistan Amended PECA in 2025 and created an Indpent Agency entitled as "National Cyber Crime Investigation Agency (NCCIA). Subsequent notification from concerned quarter established said agency in April 2025. Section 51 of ammended PECA, 2025 is being reporduced here as under:-

  - **Section 51 - Establishment of the Agency)**

    "51. Establishment of the National Cyber Crime Investigation Agency. —

    1. The Federal Government shall, by notification in the official Gazette, establish an Agency to be called the National Cyber Crime Investigation Agency (NCCIA) for the purposes of investigation and prosecution of offences under this Act.
    2. The Agency shall consist of a Director General and such number of other officers as the Federal Government may, from time to time, appoint.
    3. All powers of investigation and prosecution previously vested in the Federal Investigation Agency (FIA) under this Act are hereby transferred to the National Cyber Crime Investigation Agency upon its notification.

  - **Section 51-A Transfer and Succession of PECA, 2025**

    "51-A. Transfer of assets, liabilities, and pending proceedings. — Upon the commencement of the Prevention of Electronic Crimes (Amendment) Act, 2025, and the formal notification of the Agency:

    1. all cases, investigations, inquiries, and legal proceedings of any nature whatsoever, pending before or initiated by the defunct Cyber Crime Wing of the Federal Investigation Agency, shall stand transferred to and be deemed to have been initiated by the National Cyber Crime Investigation Agency (NCCIA);
    2. all rights, privileges, concessions, and licenses held or enjoyed by the defunct Cyber Crime Wing shall stand transferred to and be deemed to be the rights, privileges, concessions, and licenses of the Agency;
    3. all properties, assets, and records, whether physical or digital, and all liabilities and obligations of the defunct Cyber Crime Wing shall be the properties, assets, records, liabilities, and obligations of the Agency; and
    4. all contracts and agreements entered into by or on behalf of the defunct Cyber Crime Wing shall be deemed to have been entered into by or on behalf of the Agency."

Establishment

FIA CCW / NR3C was state run wing of Federal Investigation Agency (FIA). Resources required to meet the organizaqtional objectives were provided by the state of Pakisatn. Resources allocated/ alloted by the the state are financially sponsored through Agency's Budeget. NCCIA erstwhile FIA CCW promotes the cyber security interests of Sate of Pakistan at National and International Level through Rule of Law. NCCIA erstwhile FIA CCW/NR3C is full member of OIC-CERT since its first seminar in 2009 at Kuala Lampur, Malaysia. Therefore objectives of NCCIA are aligned with the objectives of OIC-CERT.

Resources

Public, National and International.

Constituency:

National and International.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- The Principal APS&C (FWO) Cobb Lines Rawalpindi requested The Director General (DG), National Cyber Crime Investigation Agency (NCCIA) to organize cybersecurity awareness session for senior wing students of said institute. The Director Admin, NCCIA deputed Muhammad Akram Mughal, Deputy Director Network Security, NCCIA and Madam Tayaba Daulat, AD Forensics NCCIA to conduct said session. Summary of the event is as under, please.

  Topic : Cyber Security Awareness Session
  Venue : APS&C (FWO) Cobb Lines Rawalpindi Auditorium
  Date : 16-02-2026
  Time : 11:00 PM to 12:30 PM

- The Principal APS&C - FWO Gracy Lines Chaklala Rawalpindi requested The Director General (DG) National Cyber Crime Investigation Agency (NCCIA) to conduct awareness session on cybercrime for the students of SSC & HSSC of aforementioned institute. The Director Admin, NCCIA deputed Muhammad Akram Mughal, Deputy Director Network Security, NCCIA and Madam Tayaba Daulat, AD Forensics NCCIA to conduct said session. Summary of the event is as under, please.

  Topic : Awareness Session on Cybercrime
  Venue : APS&C - FWO Gracy Lines Chaklala Rawalpindi Auditorium
  Date : 22-01-2026
  Time : 11:30 AM to 1:30 PM

Events involvement

- Sir Syed (SS) C@SE Institute of Technology (IT) Islamabad and International Islamic University (IIU) Islamabad co-oragnized InfoSec Summit 2026 in auditorium of Islamabad Chamber of Commerce & Industry Building on 10th Feburary 2026. Dr. Syed Jawad Hussain, Chairman, Department of Computer Science, SS C@SE IT Islamabad invited me offically as a guest speaker at InfoSec Summitt Islamabad 2026.
- Pak-Austria Fachhochschule: Institute of Applied Sciences and Technology (PAF-IAST), KP organized CySec Student Society organized TechJam 2026 Cybersecurity event, organized by the Cyber-Sec Society on 12-02-2026. The said student society offically invited Muhammad Akram Mughal, Dy. Dir. Network Security, NCCIA as a guest speaker and chief guest of above cited event.
- The Sustainable Development Policy Institute (SDPI) of Pakistan organized seminar on "The Road to Digital Safety Combating Technology Facilitated Violence against Women and Girls" dated 16-02-2026. The Executive Director SDPI Islamabad officially invited Muhammad Akram Mughal, Dy. Dir. Network Security, NCCIA as a penalist in said seminar.
- NCCIA received Eighty Five (85) Military Police Officers at her HQs in Islamabad on 12-12-2025. Muhammad Akram Mughal, Dy. Dir. Network Security, NCCIA was deputed to brief the visiting officers regarding the core functions and operations of NCCIA.
- The Sustainable Development Policy Institute (SDPI) of Pakistan organized seminar on "Securing Digital Lives: Addressing Cybersecurity and Gender-Based-Violence in Online Spaces" dated 15-12-2025. The Executive Director SDPI Islamabad officially invited Muhammad Akram Mughal, Dy. Dir. Network Security, NCCIA as a penalist in said seminar. Participipants included Policy Makers, Lawyers, Media Persons, etc.
- Ghulam Ishaq Khan Institute (GIKI) of Engineering Sciences and Technology is consistently ranked among the top 3-5 engineering universities in Pakistan. Head of Department Computer Science and Artificial Intelligence Department GIKI, Topi, Pakistan invited Muhammad Akram Mughal, Dy. Dir. Network Security, NCCIA to deliver guest lecture on "NCCIA: Contributions in National & Global Cybersecurity Index of Pakistan" dated 21-11-2025.
- Centre for Peace and Development Initiatives (CPDI) is a leading Pakistani policy and advocacy NGO that, with support from partners like the European Union, works to improve governance, promote civic rights, and foster sustainable peace and development. Executive Director CPDI requested the DG NCCIA to nominate a representative who could deliver a session on "Online Safety, Cyber Crimes and Complaint Mechanism in Pakistan". The DG NCCIA nominated Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA HQs. Islamabad to conduct requisite session that commenced 29th October, 2025 at 12:00 pm to 1:00 pm in IFQ Hotel, Islamabad.
- National Defense University (NDU) Islamabad officially invited Muhammad Akram Mughal, Deputy Director Network Security, NCCIA HQs. Islamabad to deliver lecture on "Cyber Harassment for FCS Students/Faculty/Staff". Requisite lecture was delivered on 12-11-2025 at NDU PRSA & IT Auditorium.
- The National Defense University Islamabad invited DG NCCIA to speak at the 27th National Security Workshop (NSW) held at Institute of Strategic Studies, Research and Analysis (ISSRA). The Honourable DG NCCIA deputed Mr. Muhammad Akram Mughal, Deputy Director

Network Security, NCCIA, who delivered a talk on "Media Regulations, Code of Conduct and Ethics" on 10 November 2025 to a high-level audience comprising legislators, senior civil/ military officials, and civil society representatives.

- An NCCIA Nominated Officer Conducted Trainining session on "Cyber Crime" dated 18-11-2025 at ECO Postal Staff College, G-8, Islamabad during postal management course for the probationary officers of 35th spcialized training program.
- An NCCIA Nominated Officer Conducted Trainining session on "Advanced Digital Forenics: Trends and Challenges" dated 29-10-2025 at National University of Computer and Emerging Sciences (FAST-NUCES) Islamabad: A leading Pakistani university renowned for excellence in computer science, software engineering, and IT education. Audience of session were students of MS Cybersecurity.
- An NCCIA Nominated Officer Conducted an AwarenessTrainining session on "Cyber Crimes and Remedies" dated 22-10-2025 at Institute of Business Administration (IBA) Sukkur during the Pakistan School of Internet Governance (PkSIG) 2025 Workshop.
- An NCCIA Nominated Officer Conducted an Awareness Training session on "Cybersecurity: Knowledge, Skills & Abilities by Applying NIST NICE Workforce Framework" dated 21-10-2025 at Aror University of Art, Architecture, Design and Heritage, Sukkur.
- Shah Abdul Latif University, Khairpur, Computer Science Department organized a seminar on "Cybersecurity: Knowledge, Skills & Abilities" dated 20-10-2025 by formally requesting Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA HQs. Islamabad.
- Institute of Business Administration (IBA), Sukkur, requested Mr. Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA HQs. Islamabad to conduct training session on "Network Forensic Process and Tools" dated 23-10-2025.
- National Database and Registration Authority (NADRA) Regional HQ. Sukkur requested Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA HQs. Islamabad, to conduct training session on "Cyber Laws" for her staff dated 22-10-2025.
- The National Database and Registration Authority Regional Headquarters Sukkur requested Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA, to conduct a training session on "Cyber Laws" for its staff on 22 October 2025.

2026 PLANNED ACTIVITIES

- Approval of National Cyber Crime Investigation Agency (NCCIA) Rules.
- Expansion of NCCIA at Division/District Level.
- HR Induction as per expansion Plan.
- Procurment of Latest Digital Foresnics, Network/Cyber Security and Cyber Investigations through PC-1.
- Inhouse Developlment of Special Purpose Electronic Investigation Tools.
- Implemention of concerned ISO standards (ISO 9001 and ISO 27001) in different sections of NCCIA.
- Accreditation of Digital Forensic Labs at Zonal Level from Pakistan National Accreditation Council/Concerned body.
- Robust Training Plan for NCCIA officers/ offcials serving in labs, network security and field staff.

The Principal APS&C (FWO) Cobb Lines Rawalpindi requested The Director General (DG) National Cyber Crime Investigation Agency (NCCIA) to organize cybersecurity awareness session for senior wing students of said institute. The DG NCCIA deputed Muhammad Akram Mughal, Deputy Director Network Security, NCCIA and Madam Tayaba Daulat, AD Forensics, NCCIA to conduct said session.

The Principal APS&C - FWO Gracy Lines Chaklala Rawalpindi requested The Director General (DG) National Cyber Crime Investigation Agency (NCCIA) to conduct awareness session on cybercrime for the students of SSC & HSSC of aforementioned institute. The Director Admin, NCCIA deputed Muhammad Akram Mughal, Deputy Director Network Security, NCCIA and Madam Tayaba Daulat, AD Forensics NCCIA to conduct said session.

Sir Syed (SS) C@SE Institute of Technology (IT) Islamabad and International Islamic University (IIU) Islamabad co-oragnized InfoSec Summit 2026 in auditorium of Islamabad Chamber of Commerce & Industry Building on 10th Feburary 2026. Dr. Syed Jawad Hussain, Chairman, Department of Computer Science, SS C@SE IT Islamabad invited Muhammad Akram Mughal, Deputy Director Network Security NCCIA as a guest speaker at InfoSec Summitt Islamabad 2026

The Cyber-Sec Society of Pak-Austria Fachhochschule: Institute of Applied Sciences and Technology (PAF-IAST), KP organized TechJam 2026 Cybersecurity event. The above stated society invited Muhammad Akram Mughal, Deputy Director Network Security NCCIA as a guest speker and chief guest of the TechJam 2026 event

The Sustainable Development Policy Institute (SDPI) of Pakistan organized seminar on "The Road to Digital Safety Combating Technology Facilitated Violence against Women and Girls" dated 16-02-2026. The Executive Director SDPI Islamabad officially invited Muhammad Akram Mughal, Dy. Dir. Network Security, NCCIA as a penalist in said seminar.

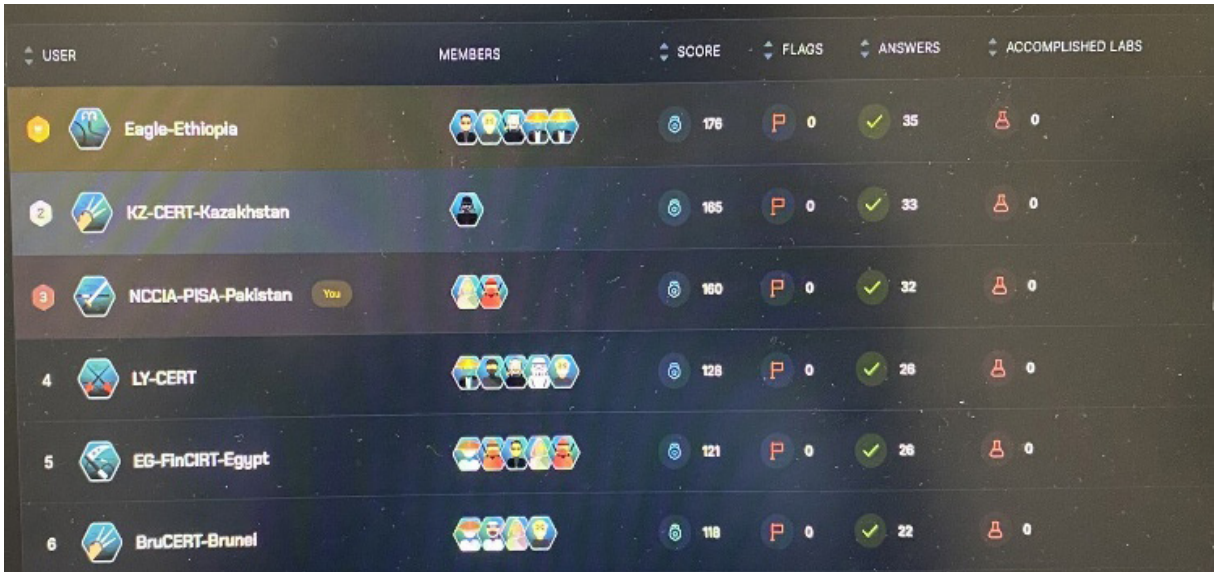
NCCIA received Eighty Five (85) Military Police Officers at her HQs in Islamabad on 12-12-2025. Muhammad Akram Mughal, Dy. Dir. Network Security, NCCIA was deputed to brief the visiting officers regarding the core functions and operations of NCCIA. Commandant, Military Police (MP) and Director Admin, NCCIA exchanged souvenirs at the end of briefing session.

The Sustainable Development Policy Institute (SDPI) of Pakistan organized seminar on "Securing Digital Lives: Addressing Cybersecurity and Gender-Based-Violence in Online Spaces" dated 15-12-2025. The Executive Director SDPI Islamabad officially invited Muhammad Akram Mughal, Dy. Dir. Network Security, NCCIA as a penalist in said seminar. Participipants included Policy Makers, Lawyers, Media Persons, etc. The following picture shows the proceedings of the SDPI seminar.

Ghulam Ishaq Khan Institute (GIKI) of Engineering Sciences and Technology is consistently ranked among the top 3-5 engineering universities in Pakistan. Head of Department Computer Science and Artificial Intelligence Department GIKI, Topi, Pakistan invited Muhammad Akram Mughal, Dy. Dir. Network Security, NCCIA to deliver guest lecture on "NCCIA: Contributions in National & Global Cybersecurity Index of Pakistan" dated 21-11-2025.

The Centre for Peace and Development Initiatives (CPDI), with support from the European Union, requested DG NCCIA to nominate a speaker for a session on online safety and cybercrime. Consequently, Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA, was nominated and delivered the session on 29 October 2025 at IFQ Hotel, Islamabad

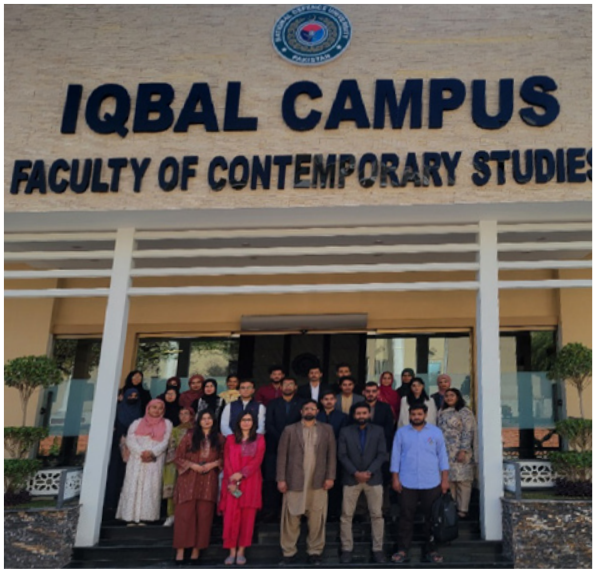
Muhammad Akram Mughal, Deputy Director (Network Security), NCCIA Pakistan, led the NCCIA team in the "13th Arab Regional, OIC-CERT & Africa Cyber Drill", held on 18 September 2025 in Rabat, Morocco. The drill was organized under the OIC-CERT framework and hosted by Morocco. Under his leadership, the NCCIA team secured 3rd position among cybersecurity teams from 57 Muslim member states, bringing significant recognition to both NCCIA and Pakistan. This achievement reflects his professionalism, dedication, and strong leadership in the field of cybersecurity.



Faculty members along with students of BESE from National University of Sciences and Technology (NUST), Military College of Signals (MCS), visited NCCIA on 19 November 2025 to gain insights into NCCIA's cybersecurity practices and operational framework.

Muhammad Akram Mughal, Deputy Director (Network Security) at NCCIA Pakistan, earned the Certified Ethical Hacker (CEH) Version 13 (V13) certification on 19 May 2025, achieving an outstanding score of 96.8% in a rigorous four-hour examination.

National Defense University (NDU) Islamabad officially invited Muhammad Akram Mughal, Deputy Director Network Security, NCCIA HQs. Islamabad to deliver lecture on "Cyber Harassment for FCS Students/Faculty/Staff". Requisite lecture was delivered on 12-11-2025 at NDU PRSA & IT Auditorium



The National Defense University Islamabad invited DG NCCIA to speak at the 27th National Security Workshop (NSW) held at Institute of Strategic Studies, Research and Analysis (ISSRA). The Honourable DG NCCIA deputed Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA, who delivered a talk on "Media Regulations, Code of Conduct and Ethics" on 10 November 2025 to a high-level audience comprising legislators, senior civil/military officials, and civil society representatives

Faculty members along with 40 students of BEIS-4 from National University of Sciences and Technology (NUST), Military College of Signals (MCS), visited NCCIA on 12 November 2025 to gain insights into NCCIA's cybersecurity practices and operational framework.

The National Database and Registration Authority Regional Headquarters Sukkur requested Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA, to conduct a training session on "Cyber Laws" for its staff on 22 October 2025.

An NCCIA Nominated Officer Conducted Trainining session on "Advanced Digital Forenics: Trends and Challenges" dated 29-10-2025 at National University of Computer and Emerging Sciences (FAST-NUCES) Islamabad: A leading Pakistani university renowned for excellence in computer science, software engineering, and IT education. Audience of session were students of MS Cybersecurity.

An NCCIA Nominated Officer Conducted an AwarenessTrainining session on "Cyber Crimes and Remedies" dated 22-10-2025 at Institute of Business Administration (IBA) Sukkur during the Pakistan School of Internet Governance (PkSIG) 2025 Workshop.

An NCCIA Nominated Officer Conducted an Awareness Trainining session on "Cybersecurity: Knowledge, Skills & Abilities by Applying NIST NICE Workforce Framework" dated 21-10-2025 at Aror University of Art, Architecture, Design and Heritage, Sukkur.

Shah Abdul Latif University, Khairpur, Computer Science Department organized a seminar on "Cybersecurity: Knowledge, Skills & Abilities" dated 20-10-2025 by formally requesting Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA HQs. Islamabad.

Institute of Business Administeration (IBA), Sukkur, requested Mr. Mr. Muhammad Akram Mughal, Deputy Director Network Security, NCCIA HQs. Islamabad to conduct training session on "Network Forensic Process and Tools" dated 23-10-2025.

PAKISTAN

PAKISTAN INFORMATION SECURITY ASSOCIATION (PISA)

HIGHLIGHTS OF 2025

Summary of Major Activities

- Co-organized national-level cybersecurity seminars and conferences.
- Conducted awareness programs and partner events across Pakistan.
- Supported PTA Cybersecurity Awareness Week nationwide.

PISA conducted conferences, seminars, awareness campaigns, and partner activities across Pakistan, focusing on national cyber resilience, AI in cybersecurity, and public-private collaboration.

Achievements

- Organized and co-organized major cybersecurity events.
- Expanded national awareness initiatives.
- Strengthened partnerships with national and international organizations.

ABOUT ORGANIZATION

Pakistan Information Security Association (PISA) is a cybersecurity think tank engaged in awareness, capacity building, conferences, and policy dialogue. It operates across major cities and conducts regular webinars, training, and international collaborations.

ACTIVITIES & OPERATION

Scope and definitions

Cybersecurity awareness, training, policy engagement, and national-level collaboration.

Incident handling reports

Community awareness and coordination support through partner initiatives.

Abuse statistics

Data not publicly disclosed.

Publication(s)

Conference materials, awareness content, and cybersecurity briefs.

New service(s)

Expanded webinar series and partner-based cybersecurity awareness programs.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

AI for Cybersecurity Conference – 13 February 2026, Islamabad (Organizer)

Events involvement

- CASS–PISA Seminar: Cyber Security – Pakistan Vision 2047 – 12 August 2025, Islamabad (Co-organizer)
- International Conference on Cyber Threat Intelligence – 11–12 July 2025, Islamabad (Collaboration partner)
- PTA Cybersecurity Awareness Week – 11–17 December 2025, Nationwide (Community CERT partner)
- Safe Secure Pakistan 2026 – 10–12 February 2026, Islamabad (Cybersecurity stakeholder)
- 13th OIC-CERT Regional Cyber Drill – 17 September 2025 (Participant Organization)
- Cyber Pakthoon week 2025- 27 -28 November 2025, Peshawar (collaboration Partner)

2026 PLANNED ACTIVITIES

- Continued national cybersecurity awareness campaigns.
- International conferences and AI-focused cybersecurity events.
- Capacity-building programs for public and private sectors.

CONCLUSION

PISA continues to play an active role in strengthening Pakistan's cybersecurity ecosystem through conferences, partnerships, awareness campaigns, and capacity-building initiatives.


RETECH
GLOBAL HSE, SECURITY AND FIRE
TECHNOLOGY CONFERENCE


Resecurity
Cyber Threat
Intelligence
Pakistan 2025
ISACA
PISA


SPIES IN THE
BITS AND BYTES


PISA
Join Collaboration
FOR 13TH REGIONAL CYBER DRI
17TH SEPTEMBER 2025
ORGANIZED BY :
NCCIA


Cybersecurity Awareness Week Closing Event - 2025
PTA Cybersecurity Awareness Week Closing Event - 2025

PALESTINE

PALCERT/GOV-SOC

HIGHLIGHTS OF 2025

Summary of Major Activities

- Data Centre Enhancement
- Join The OIC-CERT
- Strengthening The Capabilities and Enhancing the skills through training

Achievements

- Total Connected Government Entities Reached 25
- Systems And Websites Tested 24
- Number of Reported Incident Was 420
- Number of Alerts and awareness bulletin was 191

ABOUT ORGANIZATION

The Ministry of Telecommunications and Digital Economy (MTDE) is responsible for developing and regulating the telecommunications and digital infrastructure sector. The ministry plays a key role in supporting digital transformation, enhancing cybersecurity capabilities, and ensuring the resilience of national information system

The Computer Emergency Response Team (CERT) operates within MTDE and is responsible for monitoring, detecting, and responding to cybersecurity incidents affecting governmental entities and critical infrastructure.

ACTIVITIES & OPERATION

Scope and definitions

The CERT team within the Ministry of Telecommunications and Digital Economy (MTDE) is responsible for monitoring, detecting, and share awareness.
The team provides services including vulnerability reporting, and coordination with national and international cybersecurity standards.

Incident handling reports

A ransomware incident occurred on the File Server within X Organization. The affected server was promptly isolated to prevent further spread of the attack. A new server was then deployed, and clean data was restored to ensure business continuity. Also, a malware incident occurred at X Organization. The affected server was promptly isolated to prevent further spread of the threat. All malicious paths were identified and removed, and thorough checks were conducted to ensure the server was fully clean and secure before returning it to normal operation.

Abuse statistics

Incident Type	Count
Malicious IP	97
Stealth scan	171
Large traffic	36
Denied Traffic	27
Ransomware	34
CobaltStrike	13
Infected device	29
Application \host scan	205
Botnet	4
Backdoor	11
Virus	7
Exploit attempts	91

Publication(s)

Security Awareness: 126
Security Alerts: 266

New service(s)

We provide deployment and management services of XDR installation for government entities' servers hosted within our data center, ensuring continuous monitoring, advanced threat detection, and proactive incident response.

EVENTS ORGANIZED & INVOLVEMENT

Events involvement

The 10th Cybersecurity Practice, 6-7 Nov – Oman

Regional Cybersecurity Week, 28-31 Oct - Oman

Global Cyber Drill 2025, 6-8 May 2025 - Dubai

A visit to learn about the legislative, regulatory and technical environment of trust services in Lithuania

Third African Cybersecurity Forum – Kenya

2026 PLANNED ACTIVITIES

- Engagement in Palestine Cybersecurity & Artificial Intelligence Conference
- Several Project to expand the centre

CONCLUSION

The Ministry of Telecommunications and Digital Economy, through its Computer Emergency Response Team / GOV-SOC, has demonstrated steady progress in strengthening the national cybersecurity posture across government entities. The expansion of connected entities, the continuous monitoring of security events, and the effective handling of incidents.

Moving forward, sustaining this momentum will require continued investment in capacity building, expansion of monitoring coverage, and further development of governance and policy frameworks. Strengthening partnerships at both national and international levels will also remain essential to address evolving cyber threats.

QATAR

NATIONAL CYBERSECURITY AGENCY (NCSA)

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

HIGHLIGHTS OF 2025

Summary of Major Activities

- The national incident management framework (NIMF) were launched in February 2025, and the version targeting critical national organization (CNO) along with the report template was circulated to the relevant entities. Followed by awareness workshops were conducted for the implementation of NIMF.
- Sharing Information related to emerging cyber threats and vulnerabilities with entities across Qatar through official channels and NCSA's website to protect systems and digital assets. Also, identifying and taking down fraudulent domains impersonating government entities in Qatar. Responding to internal and external stakeholder inquiries through the provision of cybersecurity-related information and guidance. In addition, securing national events by delivering various cybersecurity services of NCSA. Conducting penetration testing and consultancy services to proactively identify vulnerabilities and mitigate the risk of exploitation by malicious actors.
- In 2025, the Cybersecurity Policies and Strategies Department implemented several strategic initiatives aimed at strengthening national cybersecurity governance and enhancing institutional compliance. Key activities included developing training materials related to national cybersecurity policies, standards, and guidelines, establishing the National Cybersecurity Strategy Monitoring Office, and supporting stakeholders in aligning their activities and KPIs with the national strategy.
- The Department also continued updating national cybersecurity policies, standards, and guidelines, including cloud security, vulnerability management, open-source software security, and small data center cybersecurity guidelines. In addition, the Department contributed to national and international cybersecurity engagements, capacity-building programmes, and awareness activities.

Achievements

- Publication of National Incident Management Framework.
- Launch of Secure Cyber Information Sharing (SCIS) platform to enable automated sharing of cyber threat information.
- Collaboration with Interpol to investigate and analyse malicious infrastructure.
- Establishment of the National Cybersecurity Strategy Monitoring Office.
- Conducted approximately 38 workshops with stakeholders to align activities and KPIs.

- Alignment of 60 strategic activities and agreement on 98 related KPIs.
- Delivery of around 23 specialized training courses with 361 participants.
- Development and update of national cybersecurity policies, standards, and guidelines.
- Participation in national and international cybersecurity conferences and forums.
- Support for the establishment and implementation of National Cybersecurity Academy projects.

ABOUT ORGANIZATION

The National Cybersecurity Agency aims to strengthen and regulate national cybersecurity in the State of Qatar, protect national digital assets, and support the implementation of policies, standards, and strategies that enhance cyber resilience. Through its specialized departments, the Agency works with government entities, national stakeholders, and international partners to improve cybersecurity governance, raise awareness, build national capabilities, and ensure compliance with national cybersecurity requirements.

ACTIVITIES & OPERATION

Scope and definitions

- Based on Emiri Decree No. (1) of 2021 establishing the National Cybersecurity Agency (NCSA), the Agency aims to maintain and regulate national cybersecurity and promote and protect the State's vital interests in the face of cyberspace threats. To achieve these goals, the NCSA enhances cybersecurity efforts in the State of Qatar through continuous detection, analysis, and assessment of cyber threats and incidents at the national level. It also contributes to enhancing the ability to respond quickly to cyber incidents and fostering cooperation between the public and private sectors to address security challenges, enhancing the State's readiness to deal with emergencies and ensuring business continuity and efficiency
- The Cybersecurity Policies and Strategies Department is responsible for developing, updating, and monitoring the implementation of national cybersecurity policies, standards, strategies, and guidelines. The Department also supports national entities in aligning their cybersecurity activities with national strategic objectives, enhancing compliance, and building institutional capabilities.

Incident handling reports

- 2,465 Operations reports including vulnerabilities, cyber threats and incident reports.
- 118 reported incidents.
- Conducted 17 workshops with key stakeholders, including ministries and national institutions.
- Conducted 6 internal training workshops for the Strategy Monitoring Office team.
- Conducted around 38 stakeholder workshops to support alignment of activities and KPIs.
- Aligned 60 activities with the national strategy.
- Agreed on 98 performance indicators with stakeholders.
- Issued semi-annual and quarterly progress reports.
- Launched the first stakeholder newsletter on 12 July 2025.

Abuse statistics

- Identify and taking down 549 fraudulent domains.
- The Department implemented specialized training courses covering:
  1. Policy Management.
  2. National Data Classification Policy and National Information Assurance Standard.
  3. Essential Cybersecurity Requirements for SMEs.
  4. Secure Adoption and Use of Artificial Intelligence.

A total of approximately 23 training courses were delivered, with 361 participants.

Publication(s)

- National Incident management frame (NIMF) work public Version
- National Incident management frame work CNO Version
- National Incident management frame Notification form template
- Update of Cloud Security Policy.
- Development of National Vulnerability Management Guidelines.
- Update of Open-Source Software Cybersecurity Guidelines.
- Update of Small Data Centers Cybersecurity Guidelines.
- Approval of the final version of Records Management Guidelines.

New service(s)

- Secure Cyber Information Sharing (SCIS) platform

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- Launch National Incident Management Framework

Events involvement

NCSA was involved in securing the following events:

Date	Event Name
January 2025	Trophee des Champions
February 2025	Match for Hope
February 2025	FIA World Endurance Championship 2025
February 2025	10th Substantive Session of the Open-Ended Working Group on ICT Security
February 2025	Third Senior Officials Meeting between Qatar and the EU External Action Service
May 2025	International Conference on Artificial Intelligence and Human Rights

April 2025	Moto GP25
April 2025	Lusail Multipurpose Arena Concert
April 2025	Lusail Multipurpose Arena Concert
May 2025	Circus maximus "Travis Scott"
May 2025	Arab Cub draw
May 2025	World Table Tennis Championship Elections
June 2025	INTERPOL Global Cybercrime Expert Group Meeting
July 2025	11th Substantive Session of the Open-Ended Working Group
September 2025	Panel Discussion on Data Protection in the Age of AI
September 2025	Regional Workshop on the Right to Access Information Law
November 2025	FIFA U17
November 2025	F1
November 2025	Watan Exercise
November 2025	Awareness Workshop with Al Rayan Bank
November 2025	MWC Doha 2025
December 2025	FIFA Intercontinental Cup 2025
December 2025	Arab Cup 2025
December 2025	Qatar National Day

2026 PLANNED ACTIVITIES

- Implementation of and compliance to NIMF
- Publish Vulnerability Management Guideline
- Enhancing operational services, building employee's capabilities and improving the quality of technical reports.
- Initiative to accelerates the detection, reporting, and sinkholing fraudulent domains.
- Continue implementation and monitoring of the National Cybersecurity Strategy.
- Further develop the National Cybersecurity Academy projects.
- Launch implementation of cybersecurity educational curricula in schools.
- Continue development of national cybersecurity training programmes.
- Enhance national cybersecurity research, development, and innovation initiatives.
- Continue updating cybersecurity policies, standards, and guidelines.
- Strengthen compliance monitoring related to the National Data Classification Policy.
- Continue stakeholder engagement and KPI monitoring through the Strategy Monitoring Office.

CONCLUSION

In conclusion, the National Cyber Security Agency continued its efforts during 2025 to strengthen the national cybersecurity ecosystem through developing national frameworks and policies, launching strategic initiatives, and delivering training and awareness programs. The Agency also supported national readiness and response to cyber threats while actively participating in national and international events to enhance cooperation and exchange expertise. These achievements reflect the Agency's commitment to supporting secure digital transformation and building a resilient and sustainable cybersecurity environment that protects the State's interests and future readiness.

SOMALIA

NATIONAL COMMUNICATIONS AUTHORITY (NCA)/ SOMCIRT

HIGHLIGHTS OF 2025

Summary of Major Activities

- **National Coordination:** Serves as the national focal point for cybersecurity activities.
- **Incident Response:** Manages and mitigates cybersecurity incidents at the national level.
- **Threat Prevention:** Identifies and addresses emerging cyber threats.
- **Critical Infrastructure Protection:** Safeguards national cyberspace and critical systems.
- **Awareness & Education:** Promotes cybersecurity awareness and safe online practices.
- **Capacity Building:** Strengthens capabilities through training and partnerships.
- **Monitoring & Reporting:** Ensures continuous monitoring and reporting of cyber threats.
- **Policy & Coordination:** Supports national efforts through stakeholder engagement.
- **Collaboration:** Engages with government, private sector, and international CERTs.

Achievements

Somalia's Parliament Approved the National Cybersecurity Law

The House of the People of the Federal Parliament of Somalia has officially approved Somalia's Cybersecurity Law, marking a major milestone in strengthening the country's digital security framework. The law aims to protect critical digital infrastructure, secure information systems, and enhance national cybersecurity resilience. The legislation establishes a comprehensive national framework by defining the roles of the Ministry of Communications and Technology, the technical mandate of the National Communications Authority (NCA), and the obligations of critical infrastructure operators. It also outlines mechanisms for preventing, reporting, and responding to cyber incidents, including the establishment of the Somalia Computer Incident Response Team (SOM-CIRT).

The Director General of the NCA, Mustafa Yasin Sheikh, described the approval as a significant step toward building a coordinated national cybersecurity system and enhancing preparedness against cyber threats. Similarly, the State Minister of Communications and Technology, Ahmed Osman Dirie, highlighted the law as a key pillar for protecting national interests and aligning Somalia with international standards and best practices. Overall, the Cybersecurity Law is expected to strengthen digital trust, support the growth of the digital economy, and promote effective collaboration among government institutions, the private sector, and international partners.

Implementation of Somalia's National Computer Incident Response Team (SOMCIRT)

The National Communications Authority (NCA) successfully operationalized and officially launched the Somalia Computer Incident Response Team (SOMCIRT), inaugurated by Prime Minister Hamza Abdi Barre. This marks the establishment of Somalia's first national center for coordinating cybersecurity incident prevention, detection, and response. The Director General, Mustafa Yasin Sheikh, noted that SOMCIRT was developed through national consultations to strengthen cybersecurity capacity. The Minister of Communications, Mohamed Hassan Mohamed, highlighted its role in protecting critical sectors. SOMCIRT will serve as the national hub for incident response, threat coordination, alerts, and cybersecurity awareness to safeguard Somalia's digital infrastructure.

The National Communications Authorty (NCA) Signs Strategic MOUs to Strengthen Digital Regulation and Cybersecurity Cooperation

The National Communications Authority (NCA) of Somalia has signed two separate Memoranda of Understanding (MOUs) with the Malaysian Communications and Multimedia Commission (MCMC) and CyberSecurity Malaysia, aimed at enhancing collaboration in digital regulation, technical cooperation, and cybersecurity. The agreement with MCMC focuses on cooperation in key areas such as 5G frameworks, policy exchange, and institutional capacity building, while also promoting regulatory best practices and digital sector development. The MOU with CyberSecurity Malaysia outlines joint efforts to address shared cybersecurity challenges, including incident response, threat intelligence sharing, capacity building, certification programmes, cyber diplomacy, and participation in the Global ACE country chapter. These partnerships reflect NCA's commitment to strengthening Somalia's digital ecosystem, enhancing cyber resilience, and aligning with international best practices through strategic global cooperation.



NCA and SIMAD Universityo Officially Launch Global ACE Cybersecurity Certification – Somalia Country Chapter

The National Communications Authority (NCA) and SIMAD University, in collaboration with CyberSecurity Malaysia, officially launched the Global Accredited Cybersecurity Education (ACE) Certification – Somalia Country Chapter at SIMAD Town Campus. The event brought together representatives from NCA, SIMAD University, and CyberSecurity Malaysia, marking a significant milestone in strengthening Somalia's national cybersecurity capacity through globally recognized standards and professional certification. Notably, the Somalia Country Chapter is the first Global ACE center in Africa and is set to serve as a regional hub for the Horn of Africa, reflecting a strong commitment to advancing cybersecurity education and developing skilled, ethical, and industry-ready professionals. SIMAD University emphasized its role in hosting the initiative, aligning with its mission to provide globally recognized education and equip Somali professionals with the skills needed to support the country's digital future. The NCA reaffirmed its commitment to strengthening cybersecurity governance and building a skilled workforce that meets international standards. The Global ACE framework, a vendor-neutral certification scheme developed in collaboration with government, industry, and academia, will support certification, training, and capacity-building programmes for students and professionals across Somalia and the wider region


Official Visit on Turkey's Cybersecurity and CIRT Center

The National Communications Authority (NCA), led by the Director General Mustafa Yasin Sheikh, conducted an official visit to Türkiye to strengthen cybersecurity cooperation. During the visit, the delegation engaged with the Türkiye Computer Incident Response Team (TCIRT) to explore best practices in incident response, coordination mechanisms, and national-level cyber defense operations. Discussions focused on enhancing collaboration in CIRT establishment and operations, threat information sharing, capacity building, and improving Somalia's readiness to detect, respond to, and manage cyber incidents.

ABOUT ORGANIZATION

The Somalia Computer Incident Response Team (SOMCIRT), established in 2019 under the National Communications Authority (NCA), serves as the national incident response center and the official point of contact for cybersecurity incident management in the Federal Republic of Somalia. SOMCIRT is mandated to coordinate national efforts for the prevention, detection, and response to cybersecurity incidents, in collaboration with relevant stakeholders across government institutions, the private sector, and international partners.

ACTIVITIES & OPERATION

Scope and definitions

SOMCIRT's scope covers national-level cybersecurity coordination, including prevention, detection, response, and information sharing across its constituency, which includes government institutions, law enforcement, regulators, critical infrastructure, financial institutions, ICT and telecom providers, and academia.

Within this scope, SOMCIRT delivers services categorized as:

- Reactive services (incident handling and response)
- Proactive services (threat detection and prevention)
- Awareness and capacity-building activities

Incident handling reports

SOMCIRT operates as the official contact point for reporting cybersecurity incidents, vulnerabilities, and child online abuse at the national level.

Incident handling activities include:

- Receiving incident reports from organizations and individuals
- Investigating reported incidents
- Coordinating response actions
- Providing assistance and guidance to affected parties

Reactive services explicitly cover:

- Incident analysis
- Incident handling support
- Incident coordination
- On-site incident handling

SOMCIRT also ensures continuous monitoring and reporting of cybersecurity incidents and threats to support national situational awareness and effective response coordination.

Abuse statistics

SOMCIRT maintains records of reported cybersecurity incidents and abuse cases within its constituency. These include incidents affecting public and private sector entities. The collected data supports:

- Monitoring of cybersecurity threats and incident trends
- Reporting and situational awareness
- Supporting national cybersecurity coordination efforts

Publication(s)

SOMCIRT provides cybersecurity information and guidance through its official communication channels, including:

- Alerts and warnings on emerging cybersecurity threats; and
- Awareness materials promoting safe and secure use of digital services.

These publications support national awareness efforts and promote a cybersecurity mindset.

New service(s)

SOMCIRT continues to strengthen its operational capabilities through:

- Enhancement of incident response and coordination mechanisms;
- Implementation of cybersecurity awareness campaigns;
- Delivery of capacity-building and training initiatives; and
- Strengthening collaboration and information sharing with national and international stakeholders.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

The NCA Conducted the First Cohort of Cybersecurity Certification Training for Government Staff

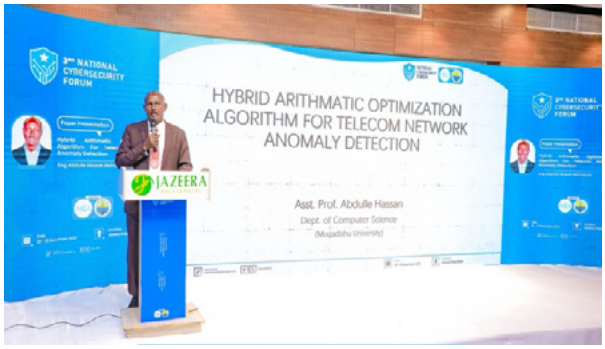
The National Communications Authority (NCA) has launched the first cohort of a cybersecurity certification training program for government staff. The initiative was inaugurated by the Director General, Mustafa Yasin Sheikh, to strengthen the capacity of IT professionals across government institutions. The program aims to enhance the protection of national digital infrastructure, improve data security, and build effective response capabilities against evolving cyber threats. The Cybersecurity Certifications covered under the program include:

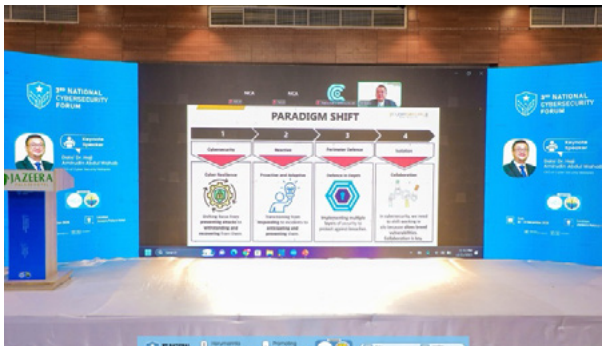
- CompTIA Security+
- Certified Incident Handler (ECIH - EC-Council)
- Cloud Security Essentials (GIAC)
- ISO/IEC 27001:2022 Lead Auditor (ISMS)
- Certified Information Security Manager (CISM) – ISACA
- Certified Information Systems Security Professional (CISSP) – ISC2

The training is delivered in Mogadishu and in Nairobi, combining flexible learning with practical experience to support the development of a skilled public-sector cybersecurity workforce.

NCA hosted Third National Cybersecurity Forum

The Third National Cybersecurity Forum was hosted by the National Communications Authority in collaboration with Mogadishu University in Mogadishu on 22–23 December 2025. Held under the theme "Promoting Digital Security in Somalia" the forum brought together key stakeholders from government institutions, the private sector, academia, and international partners to strengthen collaboration and address the country's evolving cybersecurity landscape. The event featured high-level opening remarks, expert panel discussions, and knowledge-sharing sessions focused on national priorities. The forum included technical workshops, policy dialogues, and scenario-based exercises aimed at enhancing incident response capabilities and institutional readiness. Discussions covered critical areas such as cyber threat intelligence, legal and regulatory frameworks, digital identity, data protection, and public–private partnerships. Notably, Somali cybersecurity researchers actively contributed to the forum by presenting five research papers, highlighting local expertise and innovation in the field. The event reaffirmed the leading role of the NCA in advancing Somalia's cybersecurity agenda and contributed to building a more secure, resilient, and inclusive digital ecosystem across the country.





Events involvement

NCA Hosted Safer Internet Day Event

The National Communications Authority (NCA), in collaboration with Mogadishu University, organized Safer Internet Day 2026 by hosting a national workshop under the theme: "Smart Tech, Safe Choices – Exploring the Safe and Responsible Use of Artificial Intelligence (AI)."

The workshop brought together students, academic staff, and student representatives to promote the ethical and responsible use of AI, strengthen cybersecurity awareness among Somali youth, and highlight online risks and national protection mechanisms. This initiative reflects the NCA's commitment to fostering a strong cybersecurity mindset and supporting a secure digital ecosystem in Somalia.

NCA facilited in Data Privacy Day

The Cybersecurity Department of the NCA facilitated Data Privacy Day 2026, an event organized by the National Data Protection Authority. The Director General of the National Communications Authority, Mr. Mustafa Yaasin Sheikh, attended the event and delivered key remarks. In his address, the Director General emphasized the importance of protecting personal data and highlighted the role of the NCA in advancing cybersecurity efforts. He underscored the need to develop secure and trusted digital services that benefit all Somali citizens. He further noted the shared responsibility among government institutions, the private sector, and the wider community to safeguard data, strengthen cybersecurity, and build public trust in digital systems.

2026 PLANNED ACTIVITIES

- Establish a National Cybersecurity Academy
- Strengthen SOMCIRT capabilities and enhance technical tools
- Organize the Fourth National Cybersecurity Forum
- Establish a Digital Forensics Laboratory
- Implement a National CII Compliance and Audit Program
- Deliver specialized training on cybercrime investigation and prosecution
- Conduct a nationwide cybersecurity awareness campaign across key stakeholders and communication channels
- Promote cybersecurity research and innovation

CONCLUSION

SOMCIRT plays a central role in strengthening Somalia's cybersecurity posture by coordinating national efforts in incident response, threat monitoring, and stakeholder engagement. Through its operational functions and collaboration with key national and international partners, SOMCIRT contributes to improving the security and resilience of the country's digital environment. In addition, SOMCIRT contributes to the broader Ummah and the OIC-CERT community through participation in collaborative initiatives, information sharing, and engagement with fellow member teams. This cooperation supports collective efforts to address cybersecurity challenges, enhance coordination, and promote a more secure and resilient cyberspace across OIC-CERT member states.

SULTANATE OF OMAN

OMAN NATIONAL CERT (OCERT)

HIGHLIGHTS OF 2025

Achievements

- Sultanate of Oman ranked in the 1st most cybersecurity readiness countries in the Global Cybersecurity Index (ITU)
- Awarded the Arab Excellence Award for cybersecurity innovation
- Organized the 13th Regional Cybersecurity Week in Morocco with 1500 delegates from50 countries.
- Supported the Establishments of 6 new Omani cybersecurity companies.
- Supported accreditation of 3 Omani companies through international partnerships (CREST)

Oman National CERT Hadatha Program Achievements 2021 –2025

ABOUT ORGANIZATION

In line with Oman Vision 2040 in creating an infrastructure and advanced technology that enables all sectors and is capable of absorbing the developments and challenges of cybersecurity and the attention paid by the government to economy and income diversification based on technology, knowledge and innovation as well as His Majesty direction to make the digital economy a priority and a tributary to the national economy by, the center have launched the National cybersecurity Industry Development Program "Hadatha", in 2022 which is one of the main executive programs in the National Program for Digital Economy, cybersecurity become one of the key pillar that contribute to diversifying and empowering the digital economy, which makes Oman National CERT as the first center of its kind in the in the Sultanate and globally that is specialized in cybersecurity industry development and leading national and international initiatives in this field.

Continuing to the efforts made by the Oman National CERT to enhance cooperation in cybersecurity industry development at the national, regional and global levels, it has assumed the management of the operation of the Regional Cybersecurity Centre (RCC) which was established in December 2012 in accordance to the agreement signed between the Sultanate of Oman, represented by the Ministry of Transport, Communications and Information Technology and International Telecommunication Union (ITU) , with a vision to stimulate the cybersecurity industry development ecosystem at the national, regional and global levels.

ACTIVITIES & OPERATION

Regional Level

The Regional Cybersecurity Center (RCC) presented by Eng. Badar Al-Salehi, Head of The Reginal Cybersecurity Center and the Director General of Oman National CERT delivered the opening speech at the African Cybersecurity Forum, held in Rabat from February 3–5, 2025. The Speech highlighted the importance of cooperation between the Arab and African regions, emphasizing opportunities and services that can strengthen the digital economy, particularly in the cybersecurity industry.

The Regional Cybersecurity Center collaborated with Cysec Global as the "Regional Cybersecurity Partner" for CYSEC SERIES 2025 in Qatar, Kuwait, Bahrain, UAE, Oman and as Co-Organizer for CYSEC AFRICA. RCC have conducted a capture the flag (CTF) competition in UAE through one of cybersecurity local companies "Aman" with participation of 40 participants from GCC.

Oman National CERT participated in a panel discussion during the launch ceremony of the National Framework for Cybersecurity Incident Management, organized by the National Cyber Security Agency in the State of Qatar on 23rd February 2025.

In partnership with the international CREST organization, Oman National CERT announced the accreditation of 3 Omani companies, as a significant step toward enhancing Oman's global standing in the field of cybersecurity. This achievement reflects Oman commitment to developing the capabilities of national companies, enhancing their ability to keep pace with global technological changes, and achieving international accreditations in cybersecurity and digital innovation.

The Director General of the Oman National CERT and Chairman of the OIC-CERT Board members Eng. Badar Al-Salehi delivered the keynote speech at the FDC Summit, organized by the National Telecommunications Regulatory Authority of Egypt (NTRA) and MCS Egypt on 28th to 30 April 2025 . The Event was under the patronage of Dr. Omar Tolba, Egypt's Minister of Communications and Information Technology. The speech highlighted cybersecurity's economic, diplomatic, and geopolitical dimensions, emphasized localizing the digital industry, and called for stronger Arab and Islamic collaboration.

Oman National CERT moderated a panel discussion at the FDC Summit, organized by the National Telecommunications Regulatory Authority of Egypt (NTRA) and MCS Egypt on 1st May 2025 in Egypt. The participation represented by Iman Ahmed, Director of Cybersecurity Development at Oman National CERT and Reginal Cybersecurity Center.

Oman National CERT took part in the second Global Cyber Exercise with 130 countries, held alongside the GISEC Global Exhibition in Dubai from May 5–7, 2025.

The Sultanate of Oman chaired the Board of Directors meeting of the National Centres of the Organization of Islamic Cooperation (OIC-CERT). The meeting, held on the side-line of the Regional Platform for the Digital Industry in Cairo, focused on the 2025 action plan.

Oman National CERT participated in the opening remarks at the International Conference on Information Security and Cybersecurity (CAISEC'25), under the generous patronage of His Excellency Dr. Amr Talaat, Minister of Communications and Information Technology of the Arab Republic of Egypt on 25th May 2025.

The Oman National CERT was honoured with the 'Arab Excellence' Award for its outstanding efforts in promoting innovation and cybersecurity industry development initiatives locally and regionally.

With the participation of more than 1,500 participants from over 50 countries, the 13th Regional Cybersecurity Week for 2025 kicked off in the Moroccan capital, Rabat on 15th to 19th September 2025. The event is organized by the Regional Cybersecurity Center in partnership with the Directorate General of Information systems Security (DGSSI) in the Kingdom of Morocco, the Forum of Incident Response and Security Teams (FIRST), and the Cybersecurity Centers of the Organization of Islamic Cooperation (OIC-CERT). Regional Cybersecurity Week Website: https://rcsweek.arcc.om/

Eng. Badar Al-Salehi, Head of The Reginal Cybersecurity Center and Chairman of the OIC-CERT Board participated in the Opening Session of the 13th Regional Cybersecurity Week for 2025 on 15th September 2025. "Enhancing Cybersecurity Resilience through Regional Cooperation" This session brought together an elite group of regional leaders to discuss ways of collaboration in the field of cybersecurity.

Oman National CERT moderated a Panel Discussion "AI-Powered Cyber Threats and Digital Sovereignty – A Global Diplomatic Dialogue" at the 13th Regional Cybersecurity Week for 2025 on 15th September 2025 represented by Iman Ahmed, Director of Cybersecurity Development at Oman National CERT and Reginal Cybersecurity Center. It highlighted the role of cyber diplomacy in addressing AI risks, enhancing international cooperation, and establishing reliable governance frameworks.

The 17th OIC-CERT Annual Conference and the FIRST Symposium for Arab and Africa was held during the Reginal Cybersecuirty Week 2024 on 16th September 2025 in the Moroccan, Rabat.

The Reginal Cybersecurity Center organized the 13th Regional Cybersecurity Drill for Arab and OIC Member States on 17th and 18th September 2025 with the participation of 55 experts representing National Cybersecurity Centers from 16 Arab, Islamic, and African countries. Held under the theme "Using Artificial Intelligence Technologies in Cybersecurity Defense Plans," the exercise marked a first-of-its-kind integration of AI technologies. It aimed to enhance teams' capabilities in rapidly detecting, handling, and responding to cybersecurity incidents

The Regional Cybersecurity Center in the Sultanate of Oman chaired the First Joint Meeting of Regional and International Organizations on 16 September 2025, aimed at identifying global priorities and addressing key gaps in cybersecurity. The meeting contributed to strengthening collaboration efforts to support the growth and security of the global economy.

The Sultanate of Oman chaired the Board meeting of the Directors of the OIC-CERT National CERTs members that was held on 16th September 2025, reviewing the work plan for the period 2024-2025 and approving future directions for the coming years.

A cooperation agreement was signed on 15th September 2025 between the Organization of Islamic Cooperation for National Cybersecurity Centers (OIC-CERT), chaired by the Sultanate of Oman, and the World Crest Organization, aimed at expanding collaboration in cybersecurity across OIC-CERT member countries.

At the Regional Cybersecurity Week 2025 events, the UAE Cyber Security Council was awarded the OIC-CERT Global Cybersecurity Award for National Cybersecurity Centers (2025) on 19th September 2025 in recognition of its Global Cybersecurity Exercise Initiative.

The Reginal Cybersecurity Center announced the "Call To Action" as a result of the 13th Regional Cybersecurity Week after a valuable exchange of expertise, resulting in a series of recommendations and outcomes.

Within the objectives of the Hadatha program to support national companies in cybersecurity around the world Tech Trends Company participated with the Omani Security Platform in presenting the CTF competition on the sidelines of the CYSEC GLOBAL UAE 2025 events held in the United Arab Emirates in strategic partnership with the Regional Cybersecurity Center

Oman National CERT participated in the opening discussion session titled: "Cybersecurity in the Era of the Artificial Intelligence Revolution", as part of the events of the third edition of the Arab International Conference and Exhibition on Cybersecurity 2025 in Bahrain on 5th November 2025.

Oman National CERT participated in the first Arab Cyber Drill, held under the theme 'Cross-Border Attacks,' as part of the 12th edition of the National Cyber Drill hosted by the State of Qatar.

National Level:

Under the umbrella of the Hadathah Development Initiative, and in support of the strategic vision of the Hadathah Cybersecurity Industry Program to strengthen and promote the cybersecurity industry, a strategic collaboration was undertaken with Madarek for Innovation to implement the second edition of the "Idea Industry Program."

Through a strategic collaboration between the Oman National CERT (OmanCERT) and Middle East College (MEC), the MECathon event was launched on 10th February 2025 with the participation of 20 teams. As part of the Youth Empowerment initiative, this event marks a significant step toward cultivating a dynamic cybersecurity ecosystem by enabling the transformation of innovative ideas into practical entrepreneurial solutions and market-ready products.

Oman National CERT in collaboration with the University of Technology and Applied Sciences – Muscat (UTAS) Organized Hadatha Cybersecurity Industry Development Hackathon . As part of the Hadathah Development Initiative, the event brought together 49 innovators from 165 applicants, forming 14 teams to develop advanced cybersecurity solutions. A Capture The Flag (CTF) competition, delivered by Bugbounty Oman Company, further enhanced participants' practical skills in penetration testing and vulnerability analysis.

As part of Hadatha awareness efforts, the new Electronic Transactions Law was published across our digital channels to inform the public and support its effective adoption.

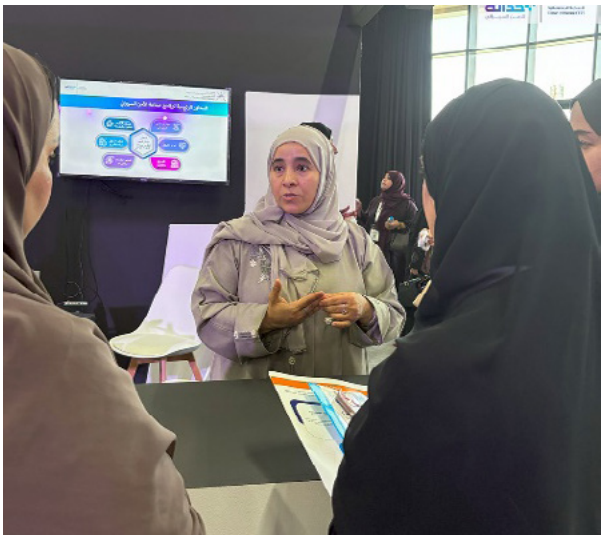
Oman National CERT held a workshop on 16th April 2025, with the participation of relevant government entities to review the Sultanate's performance in the Global Cybersecurity Index (GCI) over recent years. The session also highlighted key proposed national initiatives aimed at enhancing the country's cybersecurity readiness and strengthening its position in global rankings.

Oman National CERT participated on 16 April 2025, Muscat Collage ceremony for launching an academic cybersecurity program in—a pioneering initiative that aims to develop highly qualified national talent and supports the vision of the Cybersecurity Industry Development Program in driving economic growth.

Oman National CERT participated in World Innovation Day (21st Abril 2025) , highlighting the achievements of the Hadatha Program in promoting innovation within the cybersecurity industry Development Program.

Oman National CERT hosted a 2-day workshop for government representatives to introduce the 2025 National Cybersecurity Index Program.

Oman National CERT joined the Sixth Cybersecurity Forum (ICTS6) launch, 'Rally of the Cybersecurity Industry,' with 87+ government and key sector representatives, organized by Insight Information Security Company in partnership with the Ministry of Transport, Communications and IT from 13 – 14 Abril 2025 at Oman Active venue.



Under the patronage of His Excellency the Undersecretary of the Ministry of Transport, Communications and Information Technology for Communications and Information Technology, and in strategic partnership with Insight Information Security Company signing of several agreements to drive the wheel of economic development in the field of cybersecurity.

To enhance the capabilities of technical and executive teams in handling real-world cyber incidents, a number of cyber exercises was conducted by Oman CERT as part of the events of the Sixth Cybersecurity Forum with active participation from +87 participants from government entities on 14th May 2025.

Oman National CERT launched the 5th edition of the On-the-Job Training Program for 2025 Cybersecurity Graduates. Enhance skills and gain hands-on experience in a professional environment.

Oman National CERT launched the Cybersecurity Industry Development Program, offering services and initiatives tailored for individuals, startups, the academic sector, government entities, and the private sector and investors.

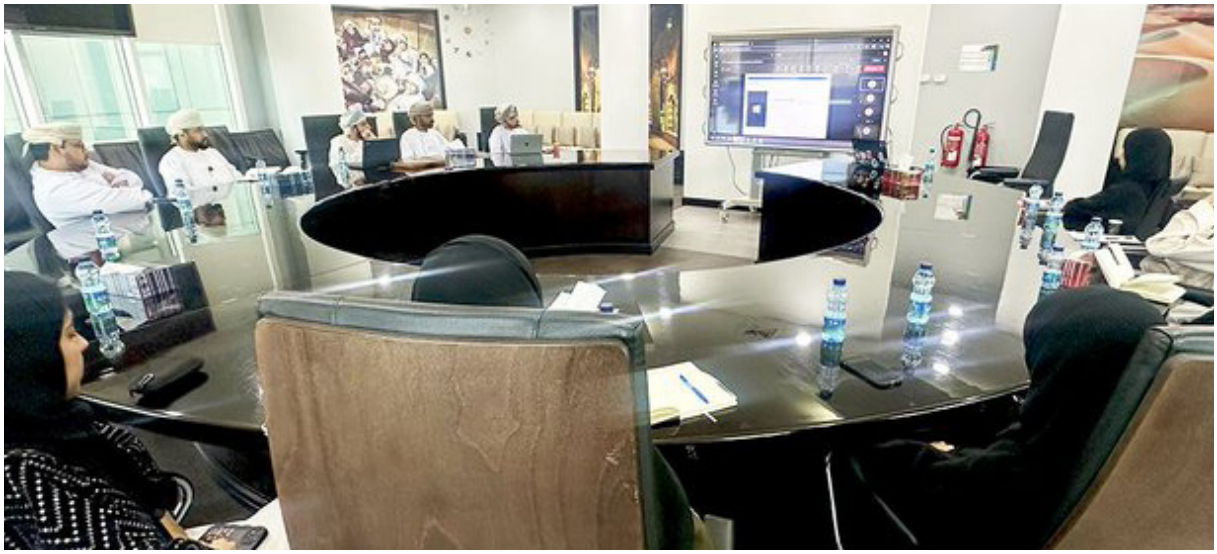
Oman National CERT launched a report for local cybersecurity companies to support the growth and expansion of local cybersecurity products and services at the local, regional, and international levels.

Oman National CERT is officially launched the "Hadatha" Cybersecurity Industry Centre at Sultan Qaboos University (SQU), under the patronage of H.E. Dr. Ali bin Amer Al Shidhani, with the aim of promoting cybersecurity research, innovation, and development.

The Sultanate of Oman participated in the 4th meeting of the Executive Committee for Cybersecurity in the Gulf Cooperation Council (GCC) states, hosted by the State of Kuwait, where the executive plan for the Gulf Cybersecurity Strategy was discussed and the recommendations of the technical committees were adopted.

With the aim of turning entrepreneurs' ideas into successful ventures, enhancing digital innovation and cybersecurity in Oman, and providing intensive training in strategic planning, digital marketing, and investment attraction, the National Centre for Information Security (Oman CERT) launched the "Pre-Incubation in Cybersecurity" program.

To follow up on the recommendations of the cybersecurity pre-incubation programme and strengthen collaboration with partners, the centre — in cooperation with the Hadatha Group — held a virtual meeting for the outputs of the Hadatha Centre and participants of the summer training programme. During the session, they presented topics including investment financing for new ventures, the startup journey, and stages of business development.



Oman National CERT participated in COMEX 2025 as part of the Ministry of Transport, Communications and Information Technology pavilion, highlighting the latest initiatives and programs in the cybersecurity sector. The event runs from 8 – 11 September 2025.

On the sidelines of COMEX 2025, the Global Cybersecurity Industry Development Watch Center — the world's first center was announced. The center aspires to be a global reference for monitoring the cybersecurity industry, enabling government and private entities to benefit from reliable data that help them develop effective strategies to address cybersecurity challenges and leverage available opportunities.

"Theqa" a secure digital identity that brings your services closer to you. It is an innovative solution launched at COMEX 2025 that makes government e-services easily accessible... wherever you are.

On the sidelines of COMEX 2025, The Oman National CERT (OCERT) organized the Hadatha Cybersecurity Forum on 10 September 2025, an interactive platform that brought together entrepreneurs, investors, and experts to discuss the latest trends in innovation and investment in the cybersecurity sector.

A Memorandum of Cooperation (MOU) was signed between the Regional Cybersecurity Centre (RCC) in Oman and CREST, aimed at advancing the national cybersecurity industry under the programme titled "Accelerating the Maturity of National Cybersecurity Companies."

A Memorandum of Cooperation (MOU) was signed between Ministry of Transport, Communications and IT and Middle East College to host Hadatha Center for the Cybersecurity Industry Development. The Hadatha Center aims to:

- Enhance the cybersecurity industry in the Sultanate of Oman
- Provide an innovative environment in cybersecurity
- Strengthen partnerships between the government sector, private sector, academic sector, and investors in the cybersecurity industry
- Address the challenges facing government and private institutions
- Develop national solutions and products in cybersecurity

'Hadatha for Excellence in the Cybersecurity Industry' initiative was taken a place at the Hadatha Conference as aside line to COMEX 2025. The winners of the Hadatha Excellence Initiative in the Cybersecurity Industry for 2025 for four categories:

- Individual Category
- Government Sector Category
- Private sector & non-profit Organization Category
- Academic Sector Category

As part of the efforts to activate Hadatha Centre for Cybersecurity Industry at Sultan Qaboos University, Oman National CERT delivered a workshop on 6th October 2025. The workshop focused on the cybersecurity industry and innovation, given by Amal Al Mushaykhi, Senior Cybersecuirty Innovation.

As part of activating the Hadatha Centre for Cybersecurity Industry at Sultan Qaboos University, Oman National CERT conducted a workshop titled: 'Freelance Opportunities in the Field of Cybersecurity' given by: Nasr Al Hadi, Cybersecurity Program Specialist. The workshop highlighted the skills and local and global platforms that enable young people to embark on this promising career path

Oman National CERT launched the 'Hadatha Centre for Cybersecurity Industry' at Middle East College on 19th October 2025 under H.E Dr. Saif bin Abdullah Al Haddabi. As part of the initiative to launch the Innovation Center for Cybersecurity Industry at Middle East College, the "Cybersecurity Challenges" page was launched to build a national base for real cybersecurity challenges, which are studied and analyzed according to technical standards under the supervision of the Oman National CERT, with the aim of developing innovative solutions that enhance the cybersecurity system in the Sultanate of Oman.

Oman National CERT announced the starting of the training program "Makeen Bootcamp" in Cybersecurity on 30 October 2025.

As part of activating Hadatha Centre for Cybersecurity Industry at Sultan Qaboos University, Oman National CERT delivered a workshop on the technical aspects of cybersecurity and AI for startups, highlighting key challenges and providing a roadmap for building secure projects using open-source tools.

Oman National CERT participated as a strategic partner in the 18th edition of CYSEC Oman 2025 on November 12, 2025. Under the patronage of Eng. Badar Al-Salehi, Director General of Oman National CERT and Head of the Regional Cybersecurity Center, where the Engineer delivered the opening address and highlighted therein Oman's strategic vision in leading the cybersecurity industry, enhancing regional and international cooperation, and adopting the Fourth Industrial Revolution technologies to support the growth of the digital economy.

Oman National CERT organized 'Hadatha Sectorial Hackathon for the telecommunications sector – a national initiative designed to strengthen technical capabilities and reinforce cybersecurity across Oman's key industries

As part of activating the Hadatha Center for Cybersecurity at the Middle East College, the Oman National CERT team conducted a series of workshops: Cybersecurity Development and Innovation Enablement and Cybersecurity & Artificial Intelligence.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- 13th Regional Cybersecurity Week 2025
- Hadatha Hackathon
- Hadatha Cybersecurity Forum
- Hadatha Excellence for Cybersecurity Industry Award Ceremony
- OIC-CERT global Cybersecurity Awards.
- Lunched 2 Hadatha Centres at Sultan Qaboos University and Middle East Collage
- Lunched Cybersecurity Industry Watch Center

Events involvement

- CYSEC OMAN 2025
- Oman National Cybersecurity CTF
- Reginal Cyber Drills
- COMEX 2025
- Makeathon Competition
- Hadatha Sectoral Hackathon for the Telecommunications Sector

2026 PLANNED ACTIVITIES

- The next phase of the Hadatha Cybersecurity Industry Program focuses on transitioning from building foundations to maximizing economic and industrial impact by enabling a comprehensive national ecosystem based on innovation, company growth, and investment attraction. This phase seeks to transform initiatives into sustainable outcomes by supporting the development of cybersecurity products and services with commercial scalability, and by enabling national companies to expand and compete in regional and international markets.

- The upcoming phase also aims to strengthen the entrepreneurship environment, connect research and development with market needs, and expand partnerships with the public and private sectors, academic institutions, and investors. This will contribute to building a more mature and sustainable national cybersecurity industry capable of supporting the digital economy and generating long-term added value.

CONCLUSION

In 2025, the Oman National CERT continued to strengthen the Sultanate's cybersecurity posture through proactive monitoring, rapid incident response, and strategic collaboration with national and international stakeholders. The year was marked by a notable increase in cyber threat sophistication; however, OCERT demonstrated resilience and readiness in mitigating risks and safeguarding critical digital infrastructure.

Key achievements included the successful handling of cybersecurity incidents, enhancement of national cyber awareness programs, and the deployment of advanced threat detection and prevention mechanisms. OCERT also expanded its partnerships across government and private sectors, reinforcing a unified approach to cybersecurity across Oman.

Furthermore, ongoing investments in capacity building, talent development, and technological innovation have positioned OCERT as a leading authority in cybersecurity within the region. These efforts align with the broader national vision for digital transformation and resilience.

Looking ahead, OCERT remains committed to advancing cybersecurity capabilities, fostering a secure digital environment, and supporting the nation's ambitions for a sustainable and technology-driven future.

Oman National CERT Website: https://linktr.ee/cert
Reginal Cybersecurity Center: https://linktr.ee/ituarcc

THE GAMBIA

THE GAMBIA COMPUTER SECURITY INCIDENT RESPONSE TEAM(GMCSIRT)

HIGHLIGHTS OF 2025

Summary of Major Activities

- **Global Cyberdrill 2025:** Participated in this event in Dubai from May 6 to 8, gaining valuable insights into international best practices in incident response and cybersecurity coordination.
- **37th Annual FIRST Conference & NatCSIRT:** Participated in these two events held between 22 and 28 June 2025 in Copenhagen, Denmark, engaging in specialized training sessions and global cybersecurity knowledge exchange.
- **ITU DFS Virtual Webinar Series:** We participated in the ITU Digital Financial Services (DFS) Webinar Series, which commenced on February 18, 2025. The series covered a range of topics focused on enhancing the security of DFS applications and protecting the broader digital financial ecosystem.
- **FIRST Africa Liaison Virtual Training:** We participated in the FIRST Africa Liaison virtual training sessions, which focused on key cybersecurity topics and helped foster regional collaboration among CERT teams across Africa.
- **Regional Cybersecurity Week 2025:** We participated in the Regional Cybersecurity Week 2025, held from 15th to 19th September in Rabat, Morocco, attending the main conference on the 15th and 16th, where experts shared experiences on consolidating and exchanging knowledge in cybersecurity, and joining the 13th Arab Regional, OIC-CERT, and Africa Cyber Drill on the 17th and 18th, conducted in a hybrid format with engaging and insightful scenarios.
- **Strengthening Cybersecurity through Effective CSIRT and SOC Models:** From 22nd to 26th September 2025, we attended this training in Nairobi, Kenya. Our participation was crucial as it provided an opportunity to acquire up-to-date knowledge and skills in key areas of cybersecurity, including threat detection, incident response, risk management, and the implementation of national cyber defense strategies. This important training was organized by the International Telecommunication Union (ITU) in collaboration with the EU Global Gateway.

Achievements

- Enhanced cybersecurity awareness among key stakeholders with FIRST in organizing first ever in-country technical training and CyberDrill.

- Improved national incident response protocols.
- Strengthened relationships with international partners.
  - Operationalized real-time threat monitoring using automated CTI platform.
  - Establishment and operationalization of DFS Security Testing Lab for android and SIM/ USSD With support from ITU.
  - Participated in key policy consultations with the Ministry of Communications and Digital Economy (MOCDE) on CII Mapping and Risking Assessment framework.
  - Signed international MoU's with Togo National CSIRT (tgCERT), CTM360, and Slovakia Nation CSIRT (SK-CERT).

ABOUT ORGANIZATION

The Gambia Computer Security and Incident Response Team (gmCSIRT), a subdivision under the Public Utilities Regulatory Authority (PURA), is tasked with:

- Providing timely advice and support on cyber threats and vulnerabilities
- Serving as the national point of contact for cybersecurity matters
- Supporting public and private sector entities, especially critical infrastructure operators
- Facilitating proactive and reactive cybersecurity services
- Strengthening collaboration with regional and international cybersecurity stakeholders

ACTIVITIES & OPERATION

Scope and definitions

At present, our operations are focused on the provision of basic reactive and proactive services. These services are primarily aimed at strengthening the situational awareness of our Constituents of National Interest (CNIs) and supporting early detection of cyber threats.

We currently utilize a Threat Intelligence Platform (TIP), to aggregate, analyse, and disseminate threat intelligence feeds to our CNIs. As of now, the platform supports 83 entities of national interest, to whom we distribute daily intelligence feeds comprising over 1,000,000 events.

The threat intelligence shared with our CNIs includes, but is not limited to:

- Malware indicators (hashes, signatures, and related artifacts)
- Malicious IP addresses and domains
- Phishing and scam campaign indicators
- Command-and-control (C2) infrastructure information
- Emerging cyber threat trends and advisories

This intelligence enables CNIs to proactively enhance their defensive measures, improve incident detection capabilities, and reduce exposure to known and emerging cyber threats.

Incident handling reports

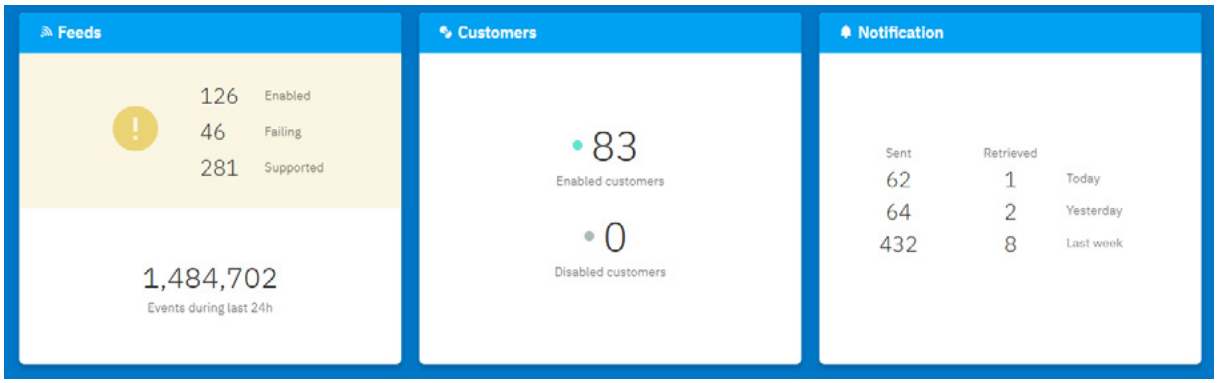


Figure 1: Real-time system metrics showing feed status, active customers, and notification activity.

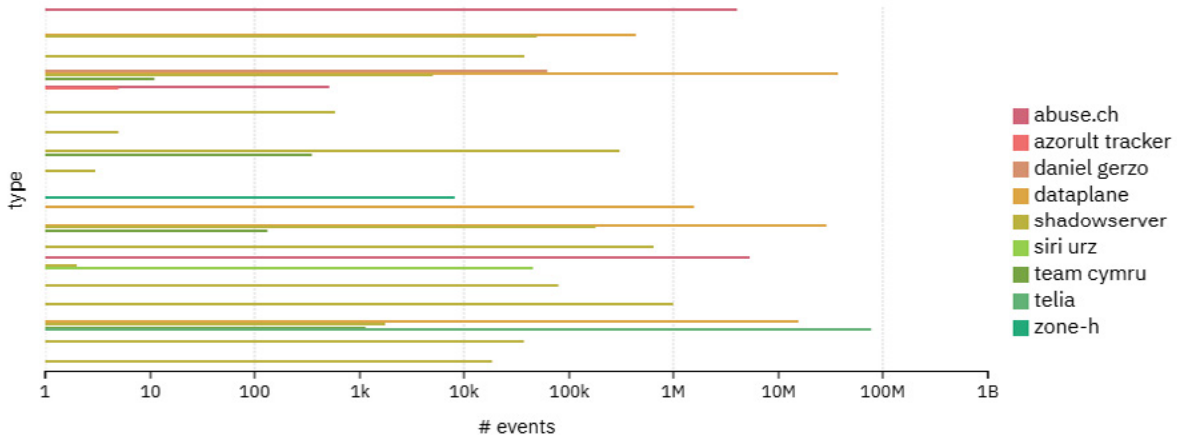


Figure 2: Overview of Collected Feed Data [4.0] – showing events grouped by feeder.

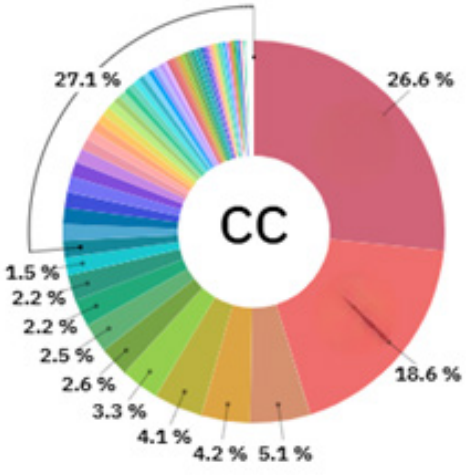
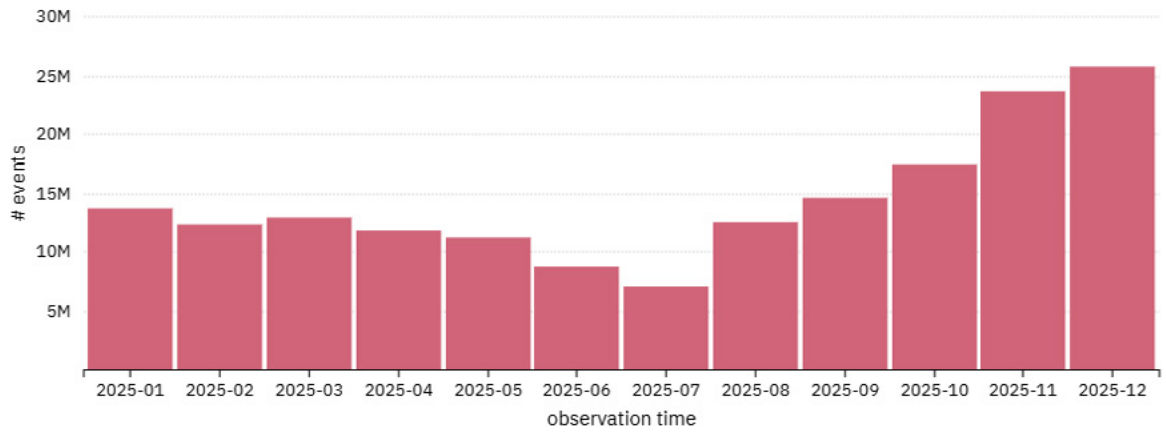


Figure 3: Overview of Collected Feed Data [4.0], showing unique IPs grouped by country code (CC)

Abuse statistics



New service(s)

Expanded webinar series and partner-based cybersecurity awareness programs.

In the course of the 2025 calendar year, we performed security audit on three MNO's DFS Android applications and SIM/USSD security testing. Additionally, we organized training for key critical institutions in The Gambia and conducted a cyber drill that helped improve their understanding, capacity, and response to cyber incidents.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

Digital Financial Services (DFS) Security Clinic

On February 4–5, 2025, gmCSIRT organized a two-day online training in collaboration with the International Telecommunication Union (ITU). This program targeted stakeholders across the DFS ecosystem, including mobile network operators, FinTechs, and banks. The sessions focused on identifying and mitigating risks in digital financial services, introducing participants to DFS Security Recommendations, Cyber Resilience Toolkits, and the ITU DFS Security Lab. The training strengthened national capacity in safeguarding financial systems and promoted adherence to global best practices.

FIRST - PURA In-Country Cybersecurity Training

From February 10–13, 2025, gmCSIRT, in partnership with FIRST and PURA, conducted a four-day national cybersecurity training. The program brought together representatives from over 70 critical national infrastructure (CNI) organizations. Participants engaged in a comprehensive curriculum covering CSIRT operations and CNI protection. The training concluded with a CyberDrill exercise, which tested incident response readiness and was highly appreciated by attendees.

Figure 4: National stakeholders during the FIRST–PURA In-Country Cyberse

Events involvement

- **Incident Response Enhancement:** Enabled better detection and faster response times through real-time alerts, coordinated response protocols, and increased automation.
- **gmCSIRT enhancement Project:** As part of the World Bank's WARDIP initiative, we collaborated with partners to finalize three key components: operationalizing gmCSIRT with clearly defined processes and roles, developing a dedicated Cyber Complaints Web Portal, and designing a National Cybersecurity Incident Reporting, Information Sharing, and Coordination Mechanism tailored to gmCSIRT's operational context. Once fully implemented, the project will significantly strengthen gmCSIRT's operational capabilities, enhance national incident detection and response, improve information sharing with stakeholders, and establish a more coordinated and resilient national cybersecurity posture.
- **Government SOC Evaluation Committee:** gmCSIRT actively contributing to the evaluation of a Government Cybersecurity Operations Center (Government SOC). As part of the implementation process, we assisted in reviewing the firms that submitted applications for the project and even identified the most qualified firm.
- **Have I Been Pwned Partnership:** On May 1st, 2025, we established a partnership with Have I Been Pwned, which granted us full and free access to data related to our government domains. This partnership has been highly beneficial, as we have integrated their APIs into our automated Threat intelligence platform. It has significantly improved our visibility and enhanced the quality of our threat intelligence feeds.

2026 PLANNED ACTIVITIES

- **International Engagement:** Expand gmCSIRT's presence and active participation in regional and global CSIRT networks.
- **National Cybersecurity Exercises:** Organize and evaluate national readiness drills to test incident response and coordination.
- **Real-Time Threat Assessments:** Further enhance monitoring and threat assessment capabilities.

- **Capacity Strengthening:** Strengthen institutional capacity through improved technology, and continuous staff skills development.
- **Cybersecurity Frameworks:** Support the development and implementation of national cybersecurity policies, frameworks, and standards.
- **Institutional Partnerships:** Formalize cooperation through the signing of a Memorandum of Understanding (MoU) with the Central Bank of The Gambia on Digital Financial Services (DFS) Security and with The Gambia Police Force on cybersecurity and cybercrime response coordination.
- **gmCSIRT Website Revamp:** Upgrade the gmCSIRT website to include a national cyber incident reporting portal and an integrated ticketing system for both Critical Information Infrastructure (CII) operators and private citizens.
- **Policy and Procedures Review:** Review and update gmCSIRT operational policies, procedures, and manuals to ensure alignment with international best practices and standards.
- **Advanced Capacity Building:** Enhance technical expertise through specialized training in areas such as advanced Digital Forensics, Malware Analysis, and Open-Source Intelligence (OSINT) etc.
- **DFS Testing Expansion:** Expand Digital Financial Services Security testing activities beyond MNO's to include iOS and all FinTechs.
- **Stakeholder Awareness and Training:** Conduct regular cybersecurity awareness sessions and technical trainings for PURA and other external stakeholders.
- **International Accreditation:** Finalize gmCSIRT's membership with the Forum of Incident Response and Security Teams (FIRST).

CONCLUSION

gmCSIRT remains committed to enhancing The Gambia's digital resilience by responding to cyber threats, building public trust in online systems, and fostering collaboration across all levels of society. The progress made in 2025 serves as a strong foundation for deepening national cybersecurity readiness.

With strengthened internal capabilities and active external partnerships, gmCSIRT is well-positioned to anticipate and counter emerging threats in 2026 and beyond.

We extend our gratitude to ITU, AfricaCERT, FIRST, OIC-CERT, and national stakeholders for their continued support. Together, we are building a safer, more resilient digital Gambia.

TUNISIA

NACS/TUNCERT

HIGHLIGHTS OF 2025

Summary of Major Activities

- Cyber Incident Response.
- Organization of several awareness sessions.
- Cybersecurity Capacity Building.
- Support for implementing national projects related to cybersecurity.

Achievements

- In 2025, the National Agency for Cybersecurity (NACS) conducted a nationwide awareness campaign targeting children in schools and youth institutions, aiming to promote cyber security and responsible use of digital technologies. Through interactive workshops, educational sessions, and practical demonstrations, the campaign addressed key topics such as cyberbullying, online privacy, and secure internet practices. Implemented in coordination with relevant ministries and educational stakeholders, the initiative also encouraged parental involvement and contributed to strengthening a culture of cybersecurity awareness among children and youth.
- NACS/TunCERT released an online guide to help internet users secure their personal data through encryption. The document is designed to raise public awareness of digital safety and encourage people to protect their computers and smartphones as cyber threats rise.
- Tunisia's Global Cybersecurity Index score was approximately 81.93 out of 100 in the most recent evaluation, reflecting its efforts in cybersecurity preparedness and governance.Based on this score, Tunisia is classified at the "Establishing" level of commitment, meaning it has developed foundations in legal, technical and organizational structures but continues strengthening capacity and cooperation measures.

ABOUT ORGANIZATION

Introduction

The National Agency for Cyber Security is in charge of coordination with the various structures involved in the field, of the supervision of the security of the information and communication systems of the public and private structures of the national cyberspace. The Decree-Law n°2023-17 of 11 March 2023 reinforced its role in capacity building, awareness raising, international cooperation, and the establishment of compliance mechanisms such as audits, classification systems, and cloud service certification, thereby positioning NACS as a key pillar of Tunisia's digital resilience and cyber governance

Establishment

According to the new legal farmework, the National Agency for Cyber Security exerts mainly the following missions

- Develop and update policies and mechanisms for the governance and security of the national cyberspace, and make them available to the relevant sectors and organizations.
- Monitor the implementation of action plans for the security of the national cyberspace concerning:
  - Proactive measures to avoid deliberate and accidental threats to the national cyberspace.
  - Preventive measures to protect against cyber risks.
  - Mechanisms for instant detection and reporting of cyber incidents and attacks.
  - Emergency response to cope with cyber attacks and mitigate their impact.
  - Rapid recovery from the effects of cyber incidents and attacks to ensure business continuity.
  - Digital investigation to diagnose incidents and determine responsibility in relation to cyber security.
- Develop and monitor the implementation of skills development programs in the field of cyber security through:
  - Participating in the development of specialized academic and professional programs in the field of cyber security.
  - Validating cybersecurity training programs and publishing them on the Agency's official website.
  - Organize specialized cybersecurity training sessions.
  - Develop and publish cybersecurity guidelines, models and guides to be adopted by public and private organizations.
  - Develop indicators to measure the national level of cybersecurity and publish dashboards periodically.
  - Carry out periodic communication and awareness campaigns in the field of cybersecurity, particularly during cyber crises.
  - Maintain a technology watch and monitor developments in the field of cybersecurity.
  - International cooperation and coordination with foreign official structures in accordance with bilateral, regional and international agreements.

Resources

The National Agency for Cyber Security departements are the following:

- General administration
- Conduct control and quality management unit
- Governance unit
- Unit according to the objectives to complete the project to focus on the information security management system

- Management of information emergency response and briefing
- Management of information systems safety technologies
- Information security audit management
- Resource Management

Constituency

National organism: Gouvernemantal, critical infrastructure, public, and private organisms

ACTIVITIES & OPERATION

Scope and definitions

Scope

The National Computer Emergency Response Team is a national-level cybersecurity entity responsible for protecting and mitigating cyber threats targeting government institutions, critical infrastructure, businesses, and individuals. Its scope includes but is not limited to:

- **Cyber Incident Response and Management**
  - Detecting, analyzing, and responding to cybersecurity incidents.
  - Coordinating incident response efforts among public and private sector organizations.
  - Providing immediate assistance in case of cyberattacks or breaches.
- **Threat Intelligence and Information Sharing**
  - Collecting, analyzing, and disseminating cyber threat intelligence.
  - Establishing partnerships with international CERTs and cybersecurity organizations.
  - Issuing alerts, advisories, and guidelines to improve national cyber resilience.
- **Risk Assessment and Vulnerability Management**
  - Conducting cybersecurity risk assessments for critical infrastructure.
  - Identifying and addressing security vulnerabilities in national IT systems.
  - Providing security recommendations and best practices.
- **Policy, Training, and Capacity Building**
  - Developing cybersecurity policies, frameworks, and best practices.
  - Conducting awareness programs, training sessions, and cyber drills.
  - Strengthening the cybersecurity skills of public and private sector professionals.
- **Legal and Regulatory Support**
  - Assisting in the development of national cybersecurity laws and policies.
  - Collaborating with law enforcement agencies on cybercrime investigations.
  - Ensuring compliance with international cybersecurity standards.
- **International cooperation**
  - Information Sharing and exchanging with regional and international entities
  - Joint Incident Response & Crisis Coordination
  - Capacity Building & Expertise

Definitions

- **Tunisian Computer Emergency Response Team (tunCERT)**
  A government-designated entity responsible for national cybersecurity incident response, risk mitigation, and coordination of cybersecurity efforts.
- **Cyber Incident**
  Any event that compromises the confidentiality, integrity, or availability of information systems, networks, or data. Examples include malware infections, denial-of-service attacks, data breaches, and unauthorized access.
- **Cyber Threat Intelligence (CTI)**
  Information about emerging cyber threats, vulnerabilities, attack methods, and threat actors, used to enhance cybersecurity defences.
- **Critical Infrastructure**
  Essential systems and assets (e.g., energy, finance, healthcare, telecommunications, and government services) whose disruption could have severe national security, economic, or public safety consequences.
- **Vulnerability**
  A flaw or weakness in hardware, software, or network configurations that can be exploited by cyber attackers to gain unauthorized access or cause harm.
- **Risk Assessment**
  The process of identifying, evaluating, and prioritizing risks to information systems and critical infrastructure, followed by mitigation planning.
- **Cybersecurity Awareness and Training**
  Educational programs designed to improve knowledge and skills in recognizing and responding to cyber threats.
- **Incident Response Plan (IRP)**
  A structured approach outlining the procedures for detecting, responding to, and recovering from cybersecurity incidents.
- **Digital Forensics**
  The process of investigating cyber incidents through the collection, analysis, and preservation of digital evidence.
- **Information Sharing and Coordination**
  The exchange of cybersecurity-related information between government agencies, businesses, and international partners to enhance collective security.

Incident handling reports

tunCERT receive incident from National (Gouvernemantal, critical infrastructure, public, and private sector) organisms and International CERTs in order to reduce the impact of incidents, resolve their causes and learn lessons to improve resilience to future attacks.

Abuse statistics

tunCERT has published 654 security advisories via its various channels on vulnerabilities and malware likely to threaten national cyberspace, describing their impact and the appropriate solutions for applying the necessary protection measures and reducing the risk of attack. In addition, tunCERT reported 413214 incidents to the various collaborators in the national cyberspace.

Publication(s)

tunCERT publishes daily and weekly news on cybersecurity (alerts, vulnerabilities, awareness publications, etc..) via its official channels:

- Website: https://www.ancs.tn/
- Facebook: https://www.facebook.com/ansitn
- Linkedin: https://www.linkedin.com/in/ancs-tuncert-80bb4b172/
- X: https://x.com/ATuncert.

New service(s) : N-Cloud and G-Cloud labeling service

The N-Cloud and G-Cloud labeling service is a national certification framework designed for Tunisian cloud service providers to ensure compliance with cybersecurity standards and regulatory requirements.

This labeling scheme aims to:

- Strengthen the security and resilience of cloud infrastructures
- Ensure the protection of sensitive data hosted within cloud environments
- Promote trust in cloud services such as SaaS, PaaS, and IaaS

By adhering to N-Cloud and G-Cloud requirements, providers demonstrate their commitment to robust cybersecurity practices, data protection, and operational transparency.

Furthermore, the labeling contributes to reinforcing digital sovereignty, ensuring that national institutions benefit from secure, reliable, and locally compliant cloud services aligned with Tunisia's regulatory and strategic objectives

EVENTS ORGANIZED & INVOLVEMENT

Events organised

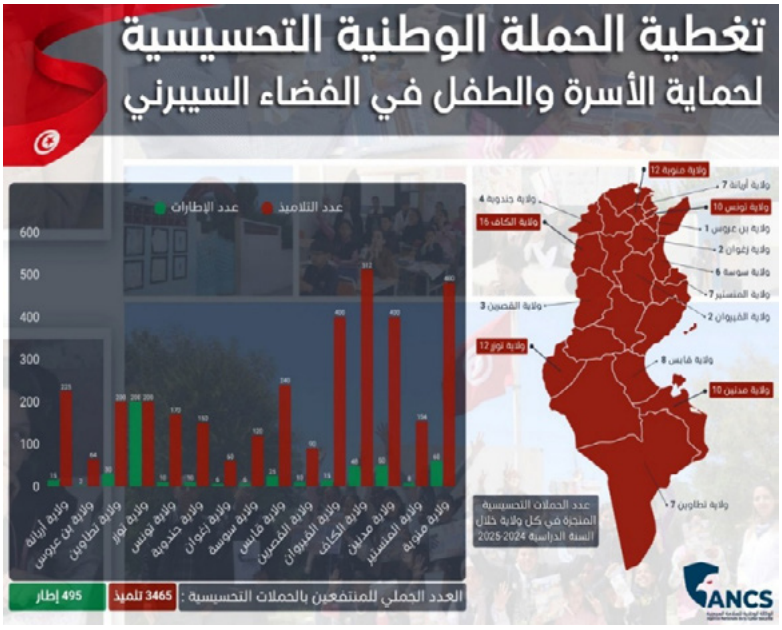
National Forum on Online Child Protection

Events involvement

- Seminar on Cybercrime: "Challenges and Responses" at the Headquarters of the General Directorate of the National Guard on January 15, 2025
- I-PROTECT V7 SENIOR

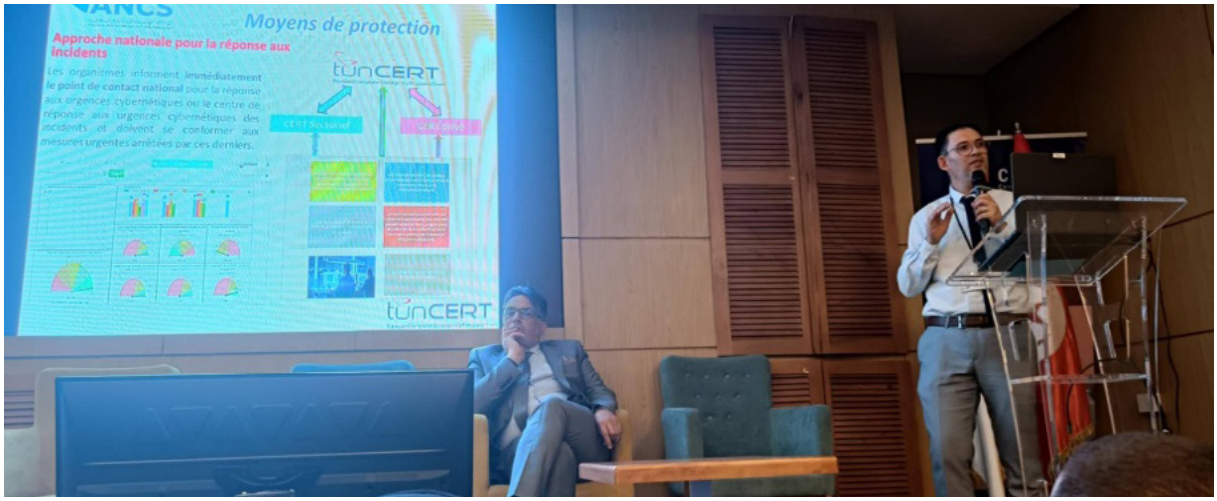
- Second edition of the international seminar on the Multi-transition organized by the Sfax Digital Research Center (CRNS): Event titled "Cybersecurity: Understanding, Protecting, and Anticipating," held at ISSBAT
- Tunisia Digital Summit: Activities of the study day on cybercrime: challenges and ways to combat it, organized by the Center for Legal and Judicial Studies under the supervision of the Ministry of Justice
- "World Tour – Tunis" event on May 21, 2025, organized by Trend Micro on the theme "Cyber Risk and Proactive Security."
- Activities of the 8th Session of the Mediterranean University for Youth and Global Citizenship
- Participation in an awareness-raising workshop on "Strengthening Capacities for Protection and Prevention of Violent Extremism and Cyber Threats."
- Training Program for Students of the 18th Cohort of the Institute of Management Leadership
- Awareness Day on Protecting Financial Institutions from Cyber Risks, organized by the Banking and Financial Council – July 2025
- National Cybersecurity Strategy 2026–2030 at the headquarters of the Banking and Financial Council – September 2025
- I-PROTECT V8 Kids in Sfax
- The Association for Development and Citizenship at the Batah Youth Center organized a regional seminar titled "The Tunisian Administration and Cyber Challenges" in Jendouba
- Organization of an awareness-raising day on the importance of cybersecurity and data protection for approximately 40 students at the Higher Institute of Technological Studies in Tozeur
    - Participation in the annual Digital Twinning Conference organized by the National Center for Educational Technologies
    - Organization of an awareness session on protection against cyber risks and threats and methods of prevention for the General Association of Retirees.
    - Participation in the activities of the Science Camp on Cybersecurity in Tozeur
    - Participation in the regional symposium on "Cyber Violence Against Women," organized by the Regional Delegation of Culture in Gabès,
    - Participation in the Presentation Day on the National Cybersecurity Strategy 2026–2030
    - Participation in the first Arab cyber exercise organized by the National Agency for Cybersecurity in the State of Qatar
    - Participation in the Arab and Global Cybersecurity Summit in the Kingdom of Bahrain
    - Participation in the Symposium FIRST & AfricaCERT 2025: Africain and Arab regions

Children awareness campaign



Participation in the Presentation Day on the National Cybersecurity Strategy 2026–2030

Incident Response Coordination with the financial Sector



Awareness session for academic universities

Participation on the Activities of the second regular session of the Council of Arab Cyber Security Ministers

Participation in the first Arab cybersecurity exercise hosted by the State of Qatar, in implementation of the resolutions adopted during the first session of the Arab Ministers of Cybersecurity Council.

Participation in the Symposium FIRST & AfricaCERT 2025 Africa and Arab region In Mauritius

2026 PLANNED ACTIVITIES

- Collaborating with both local and international cybersecurity organizations by establishing formal partnerships, including Memoranda of Understanding (MoUs) and other cooperative agreements
- Organization of awareness sessions for national establishment.
- Organization of a second edition of National Forum on Online Child Protection. Organization of a national cyber drill.

CONCLUSION

By advancing its capabilities in incident response, threat intelligence exchange, vulnerability management, and awareness campaigns, tunCERT has continued to enhance its effectiveness in anticipating and countering cyber threats. Its strong partnerships with government bodies, private organizations, and international stakeholders have been essential in mitigating risks and building greater resilience.

NACS/TunCERT remains committed to strengthening cooperation with international partners to enhance collective efforts in securing the global cyber environment. In alignment with the African, Arabic and global vision of fostering a safe, trusted, and resilient cyberspace.

Consistent with its strategic priorities—focusing on capacity and capability development, effective threat mitigation, and international engagement—TunCERT continues to advance and refine its cybersecurity frameworks, technologies, and operational processes. It also strives to drive innovation and act as a catalyst for the growth of the national and regional cybersecurity ecosystem.

UNITED ARAB EMIRATES

UAE CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

HIGHLIGHTS OF 2025

Summary of Major Activities

The UAE Cyber Security Council (CSC) strengthened national and international cyber security cooperation through active engagement in global and regional forums, multilateral discussions, and cross-border coordination initiatives. CSC broadened its cyber-diplomatic outreach by working with partners across North America, Europe, Asia, Africa, and the Middle East, while simultaneously expanding nationwide cyber awareness through targeted workshops, training sessions, and community-focused capacity-building programs. In parallel, CSC continued to play a central national role in monitoring and detecting cyber threats, supporting threat analysis, coordinating incident response activities, and working with relevant stakeholders to ensure that incident response plans across government and critical sectors remained robust, tested, and effective. CSC also elevated the UAE's profile by hosting major international gatherings, including the UAE National Cyber Governance Summit, GISEC, GITEX, CyberQ, and the Meridian Conference, through which the UAE led discussions on cyber policy, quantum and post-quantum security, and artificial intelligence security.

A major milestone of the year was the publication of the UAE National Cyber Security Strategy 2025–2031, which set the long-term national vision and strategic priorities for cyber security. CSC complemented this effort by issuing supporting mandates and regulatory enhancements, including thirteen new cyber security policies aligned with international best practices and designed to support the secure adoption of emerging technologies. These efforts strengthened national cyber governance, clarified responsibilities across stakeholders, and reinforced a consistent and coordinated approach to cyber security implementation.

CSC also advanced national cyber readiness and operational preparedness by delivering sector-wide cyber exercises, including national drills conducted across all Emirates and at major global and local events. These exercises enhanced incident response capabilities, validated technical and organizational readiness, and strengthened coordination among government entities, critical infrastructure operators, and private-sector partners. In addition, CSC led the Global Cyber Drill 2025 in partnership with the International Telecommunication Union (ITU), bringing together cyber security authorities and CERTs from around the world to simulate cross-border cyber incidents, elevate operational collaboration, and reinforce the importance of public–private partnerships in responding to large-scale and complex cyber threats.

CSC also advanced cybersecurity innovation through the CyberE71 initiative, strengthening the national startup ecosystem and fostering collaboration between government, industry, and academia to support long-term cyber resilience.

A Quantitative Summary Highlighting CSC's Achievements and Impact in 2025:

- Engaged with more than **130 countries** throughout 2025, strengthening international cooperation and expanding the UAE's global cyber security footprint.
- Conducted over **400 workshops** and technical sessions across national and international platforms, advancing capability-building and enhancing operational readiness across sectors.
- Achieved a total of **16 Guinness World Records** over the past year, reaffirming the UAE's global leadership in cyber security awareness and capacity development.
- Expanded its international cooperation framework by formalizing more than **30 Memorandums of Understanding** with regional and global partners.
- Reached **millions** through awareness efforts across the UAE, reflecting the Council's extensive outreach and its commitment to building a cyber-resilient society through sustained large-scale initiatives.

Achievements

Over the course of 2025, the UAE Cyber Security Council was formally recognized through a series of notable awards and honours, affirming its role as a leading institution in global and regional cyber security advancement:

- **OIC-CERT Global Cyber security Award 2025:** CSC was awarded with the Global Cyber security Award by the OIC-CERT for conducting the ITU Global CyberDrill 2025.
- **CAISEC'25 Recognition:** CSC was honoured during the CAISEC'25 Conference in recognition of its active role in supporting the Cyber Security ecosystem and in fostering Arab and international cooperation to combat cyber threats.
- **GISEC Guinness World Record 2025** recognizing the largest attendance at a cyber security event.
- **GISEC Guinness World Record 2025** honouring the most nationalities represented in a cyber capture-the-flag (CTF) competition.
- **GISEC Guinness World Record 2025** celebrating the most nationalities participating in a cyber security awareness lesson.
- **GISEC Guinness World Record 2025** marking the largest participation in a ransomware cyber security training session.
- **GISEC Guinness World Record 2025** distinguishing the most nationalities engaged in a simulated Dark Web intelligence training session.
- **GISEC Guinness World Record 2025** recognizing the most nationalities participating in a cyber drill competition.

- **GISEC Guinness World Record 2025** honouring the most nationalities taking part in a ransomware awareness lesson.
- **GISEC Guinness World Record 2025** celebrating the largest cyberbullying lesson.
- **GISEC Guinness World Record 2025** marking the highest number of participants in a gamified cyber security training session.
- **GISEC Guinness World Record 2025** distinguishing the most nationalities represented in a gamified cyber security training session.
- **GISEC Guinness World Record 2025** recognizing the largest ransomware awareness lesson.
- **CyberQ Guinness World Record 2025** confirming the largest postquantum cryptography lesson.
- **CyberQ Guinness World Record 2025** honouring the largest attendance at a quantum computing conference.
- **CyberQ Guinness World Record 2025** certifying the largest cryptography lesson.
- **CyberQ Guinness World Record 2025** commending the most nationalities participating in a post-quantum cryptography lesson.
- **CyberQ Guinness World Record 2025**, confirming the largest AI cyber security operations lesson.
- **Regional Arab OIC and Africa Cyber Drill in Rabat 2025**, completing 13th Regional Arab, OIC, and Africa Cyber Drill lab with a Score of 100%
- **The Defense Critical Infrastructure Conference in Azerbaijan 2025** achieved second place in cyber drills and penetration testing

ABOUT ORGANIZATION

The UAE Cyber Security Council is the government entity responsible for supporting the United Arab Emirates' efforts to achieve a secure and resilient digital transformation. Led by His Excellency Dr. Mohammed Hamad Al Kuwaiti, the CSC brings together a wide range of federal, international, local and sectoral authorities to coordinate and strengthen national cyber security readiness. The Council works closely with strategic partners across government, industry, academia and international organizations to enhance cyber capabilities and promote best practices, advancing the UAE's leadership in global cyber security development.

aeCERT was established by Decree 5/89 of 2008 issued by the Ministerial Council for Services. The Cyber Security Council was established by the UAE Cabinet in November 2020.

ACTIVITIES & OPERATION

Scope and definitions

Cyber Drills

The Cyber Drills team continued to play a critical role in strengthening national and sector-wide cyber security resilience through real-world exercises. In 2025, a total of 15 cyber drills were conducted, with a focus on enhancing operational readiness, validating cyber response capabilities and strengthening coordination among stakeholders to address increasingly complex cyber threat scenarios. Throughout the year, the CSC conducted more than 10 Capture the Flag exercises and held more than 60 activities, covering 8 vital sectors across the UAE.

1. **The Cyber Drills team operated across five key areas to achieve its mission:**
   - Scenario Development
   - Designed and delivered realistic cyber-attack scenarios reflecting contemporary threats, including large-scale incidents and advanced persistent threats.
   - Tailored scenarios to national priorities, critical infrastructure and emerging risk domains.
2. **Technology Integration**
   - Leveraged advanced cyber ranges, simulation platforms and technical environments to support realistic and high-impact exercises.
   - Integrated technical and decision-making components to reflect real operational conditions.
3. **Facilitation and Moderation**
   - Engaged experienced facilitators and moderators to guide cyber drills.
   - Conducted structured debriefings and post-exercise assessments to capture lessons learned and areas for improvement.
4. **Logistics and Infrastructure Support**
   - Coordinated end-to-end planning, execution and hosting of cyber drills across multiple formats and scales.
   - Supported both in-person and hybrid exercise models.
5. **Industry and Government Participation**
   - Enabled participation from all types of entities (governmental, critical infrastructure operators, international partners, etc.).
   - Strengthened cross-sector and cross-border collaboration to enhance collective cyber resilience.

Global Eminence

The Global Eminence team continued its mandate to position the CSC as a globally recognized leader in cyber security. The team focused on strengthening international engagement, enhancing CSC's global visibility and contributing to global cyber security dialogue through strategic partnerships and high-profile platforms. Over the past year, the CSC has secured more than 30 Memorandums of Understanding with local and global partners and conducted more than 480 meetings with global national and private entities. The Global Eminence team operated across four key areas to achieve its mission:

1. **Awards & MoUs**
   - Supported and advanced international and regional cyber security award initiatives.
   - Engaged in strategic partnerships with local and global organizations through Memorandums of Understanding (MoUs).
2. **Cyber security Events**
   - Organized UAE level Cyber Governance Summit, bringing together national leaders and cyber security experts to launch the national cyber fabric, highlighting strategic initiatives and reinforce the UAE's commitment to a secure, resilient digital ecosystem.
   - Led and supported high-impact cyber security events and conferences, including global and regional platforms hosted in the UAE.
   - Enabled strategic engagement with policymakers, industry leaders and international organizations.
3. **Thought Leadership Publications**
   - Contributed to policy discussions, position papers and strategic insights on emerging cyber security topics.
   - Promoted global best practices and future-oriented cyber security perspectives.
4. **Special Interviews & Media Engagement**
   - Supported media engagements and strategic communications highlighting CSC leadership and initiatives.
   - Amplified the UAE's cyber security narrative through international and regional media channels.

Awareness for Society

The Awareness Team continued its efforts to educate society on cybersecurity best practices and promote safe digital behaviour, strengthening public resilience against cyber threats. Through structured awareness initiatives, targeted workshops, and partnerships, the team supported the development of a cyber-aware society across diverse demographics and personas. Notable initiatives included the 52 Weeks of Awareness Campaign, which delivered weekly thematic content and awareness materials, and the Scam Busters national awareness campaign, together reaching millions across the UAE. These efforts were complemented by specialized workshops, dedicated awareness programs for women with more than 300+ participants, and the development of 13 modular awareness content tailored to different audience needs.

The Awareness Team operated across four key areas to achieve its mission:

1. **Content Development & Expertise**
   - Developed targeted cyber security awareness content aligned with national priorities and emerging risks.
2. **Outreach & Engagement**
   - Utilized digital platforms, social media and newsletters, as well as online channels to disseminate cyber security awareness messages.
   - Collaborated with public and private sector partners to extend reach and impact.
   - Delivered awareness sessions aligned with national strategies and cyber security policy developments.

3. **Event Support & Community Initiatives**
    - Supported and participated in cyber security awareness events, public initiatives, community-focused engagements and more.
4. **Cyber security Roadshows & Interactive Learning**
    - Delivered interactive and experiential learning initiatives designed to engage youth, parents and professionals.
    - Promoted practical understanding of cyber security risks and safe digital practices.

Cyber Future Leaders

The Cyber Future Leaders team focused in 2025 on strengthening cyber security leadership and strategic decision-making among senior executives and CISOs. The team aimed to enhance executive-level cyber maturity and promote informed leadership to support effective governance of cyber security risks across critical sectors, reaching more than 1,000 leaders through initiatives conducted and events organized. The Cyber Future Leaders team operated across four key areas to achieve its mission:

1. **Executive Leadership Programs**
    - Designed and delivered structured programs tailored for CISOs and senior executives.
    - Addressed strategic cyber security leadership, governance and accountability at the executive level.
2. **CISO Engagement & Peer Exchange**
    - Facilitated closed-door forums, roundtables and peer discussions for CISOs and security leaders.
    - Enabled the exchange of experiences, challenges and best practices across sectors.
3. **Strategic Awareness & Decision-Making**
    - Focused on enhancing executive understanding of emerging cyber risks and regulatory developments.
    - Supported improved decision-making through scenario-based discussions and expert-led sessions.
4. **Partnerships & Executive Ecosystem Development**
    - Collaborated with national and international partners to deliver high-impact executive-focused initiatives.
    - Strengthened the cyber security leadership ecosystem through sustained engagement with senior stakeholders.

CyberE71

CyberE71 is an initiative operating under the umbrella of the UAE Cybersecurity framework, with a vision that aligns closely with the UAE Centennial 2071 objectives. The initiative aspires to position the United Arab Emirates as a global hub for cybersecurity startups by fostering innovation and entrepreneurship within the sector. CyberE71 focuses on identifying promising ideas from young founders and cybersecurity specialists, providing them with the necessary support, guidance, and resources to transform these ideas into scalable and sustainable startup ventures that contribute to the nation's long-term digital resilience and economic growth. In 2025, CyberE71 made significant progress toward these goals, achieving key milestones that demonstrate its growing impact on the national cybersecurity innovation ecosystem.

- 3 startups have been funded and in growing and scaling.
- 60+ startups have joined the UAE Cybersecurity Innovation Challenge
- 500+ startups targeted to be in AWS Cybersecurity Accelerator Program
- 50+ startups have joined Google Accelerate AI First Demo
- 270+ applications were registered in the AI & Cyber Winter School with Google.org & Khalifa University
- 35+ partners are in the program ecosystem that includes Industry, Government, Hyperscale's & VCs
- 15+ MOUs have been signed with leading partners
- 35+ universities are participating and supporting CyberE71
- 5000+ individuals have benefited from CyberE71 Sessions
- 30+ startups will be incubated in the program.
- 22+ startups are within CyberE71 Cohorts
- 1000+ hours of mentorship has been conducted with Startups
- 200+ applications were received from Startups to Join CyberE71
- 10M+ views in CyberE71 Social Media
- 4.4M+ reach in CyberE71 Social Media

Incident handling reports

The UAE Cyber Security Council (CSC) follows a robust incident handling process that logs, assesses, and classifies all reported incidents, coordinates response and remediation actions, and documents all activities throughout the incident lifecycle. Root cause analysis and corrective measures are captured in the incident handling report, and incidents are formally closed after CSC validation and review.

Abuse statistics

The UAE Cyber Security Council (CSC) 2025 Advisory and Threat Intel Alerts Statistics:

In 2025, shared advisories and threat intelligence advanced through greater collaboration and faster information sharing, highlighting trends such as perimeter device vulnerabilities, sophisticated phishing, persistent ransomware, and the rise of PhaaS platforms—emphasizing the need for proactive threat detection and timely patching.

Advisories:

Vulnerability	3,156
Ransomware/Malware/APT	34
Awareness (Phishing, General)	109
Industrial control systems (ICS)	34
Web defacement	2163
Total	**5,496**

Threat Intel Alerts:
Total: 598

Publications

In 2025, the Cyber Security Council advanced the national cyber security posture by developing, issuing, and updating key policies, frameworks, and standards. These efforts strengthened governance, enhanced resilience, and ensured the secure adoption of emerging technologies across government and critical sectors.

On the other hand, as part of its knowledge-sharing and threat intelligence efforts, the CSC released comprehensive UAE Cyber Threat Landscape reports in partnership with Fortinet and Mastercard, providing data-driven insights into evolving threat trends, attacker behavior, and sector-specific risks affecting the UAE's digital ecosystem.

1. National Cyber Security Strategy (2025-2031)

The Cyber Security Council issued the (UAE) National Cyber security Strategy (2025-2031), the national strategy is a comprehensive framework designed to safeguard the nation's digital infrastructure, protect businesses, and ensure the safety of individuals in an increasingly interconnected world. The strategy aims to strengthen national cyber resilience, enhance digital trust, and foster innovation while mitigating cyber security threats.

2. Issuance of New National Policies

The Cyber Security Council issued new national policies to address emerging risks and evolving operational needs:

- National Cyber Security Policy for Artificial Intelligence
- National Data Exchange Security Policy
- National Encryption Policy
- National Secure Remote Work Policy
- National Third-Party Security Policy
- National Vulnerability Disclosure Policy

3. Update of National Policies, Frameworks, and Programs

The Cyber Security Council updated several existing national mandates to ensure continued relevance and effectiveness:

- National Cyber Security Governance Framework
- Critical Information Infrastructure Protection (CIIP) Policy
- National Cyber Accreditation Program
- Cyber Incident Response Framework
- Cyber Incident Response Plan
- Cyber Security Information Sharing Framework
- National Cloud Security Policy
- National Internet of Things (IoT) Policy
- SOC Baseline Capabilities

4. Refreshed UAE IA Standard

- UAE Information Assurance Standard V 2.1

5. UAE Cyber Threat Landscape Reports:

- Fortinet – UAE Cyber Threat Landscape Analysis 2025: Technical threat report analyzing cyber campaigns targeting the UAE during the first half of 2025, highlighting attacker tactics, ransomware activity, botnet behavior, and large-scale reconnaissance operations, based on anonymized security telemetry.
- Mastercard – UAE Cyber Threat Landscape Analysis: strategic threat landscape report examining attack trends, targeted sectors, threat actors, and attack methods across the UAE, with a focus on financial services, technology, and public sector risks, supported by Mastercard Cyber Insights data.

The policies, frameworks, and standards issued and updated by the Cyber Security Council in 2025 represent a significant step forward in reinforcing national cyber security governance and operational readiness. Collectively, these initiatives support secure digital transformation, improve coordination across stakeholders, and enhance the nation's ability to prevent, detect, and respond to cyber threats. The aforementioned efforts were further complemented by the publication of the UAE Cyber Threat Landscape reports developed in partnership with Fortinet and Mastercard, which provided data-driven insights into evolving threat trends and informed both policy development and operational decision-making across the national cybersecurity ecosystem.

New service(s)

1. National Information Assurance (NIA) Platform

- In Dec 2025, the Council officially launched the UAE's National Information Assurance (NIA) Platform, a sovereign AIpowered system that delivers a unified, realtime view of national cyber readiness across government and critical infrastructure entities.
- By integrating compliance, threat intelligence, risk assessment, and resilience analytics into a single platform, NIA shifts the nation from periodic reviews to continuous cyber assurance.
- With AIdriven insights, automated reporting, objective assessments, and rapid remediation workflows, the platform strengthens national resilience and supports the UAE's leadership in cyber governance.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

National Cyber Governance Summit 2025

The National Cyber Governance Summit 2025, organized by the UAE Cyber Security Council, convened more than 700 attendees from 500+ organizations, bringing together national leaders, experts, and innovators to advance the UAE's secure and resilient digital ecosystem. The Summit featured broad governmental participation and showcased the UAE's Cyber Fabric, highlighting key national initiatives including the National Cyber Security Strategy 2031, National

Cyber Security Policies, UAE Information Assurance Standard, National Information Assurance Platform, National Cyber Accreditation Program, and the National Cyber Index.

GISEC 2025

GISEC 2025 was one of the most significant cyber security events organized by the UAE Cyber Security Council. The event brought together more than 20,000 cyber security leaders, experts and organizations from 160+ countries to discuss emerging threats, innovative solutions and best practices in cyber security.

GITEX 2025

At GITEX 2025, the CSC maintained a prominent presence to showcase national cyber security initiatives and engage with global technology leaders. The CSC facilitated strategic engagements across government and industry by conducting more than 25 sessions and meetings and supported innovation dialogue and advanced partnerships aligned with secure digital transformation by signing 22+ Memorandums of Understanding.

Global Cyber Drill 2025

The Global Cyber Drill 2025 was conducted under CSC strategic oversight to test and enhance international cyber incident response and coordination. The drill engaged more than 260 participants, involving 130+ countries across 6 continents and achieving 11 Guinness World Records. In partnership with ITU, the drill involved multiple countries and organizations, simulated complex threat scenarios and supported executive-level decision-making exercises. CSC led scenario governance, partner coordination and outcome evaluation.

CyberQ 2025

CyberQ 2025 was one of the UAE's leading strategic cyber security events organized by the CSC, witnessing an attendance of 2850+ participants. The event convened senior government and industry stakeholders, global experts and practitioners to address emerging priorities in cyber security, focusing on post-quantum security and artificial intelligence. As part of its technical program, CyberQ featured a hackathon that culminated in 8 winning teams receiving awards from a prize pool of AED 100,000. The event also achieved 5 Guinness World Records, further underscoring its global significance and facilitated the signing of 15 Memorandums of Understanding with key regional and international partners to strengthen strategic cyber security collaboration.

Meridian Conference

The Meridian Conference was a strategic cyber security policy event organized by the CSC. The conference convened policymakers and international experts to discuss global cyber security governance and policy alignment, reinforcing the UAE's role in advancing international cyber security dialogue. The 2025 edition brought together 30+ delegates from 20+ countries and featured 10+ specialized sessions, underscoring the event's growing influence as a premier platform for multilateral cyber security collaboration.

Digital Shield: A Cybersecurity Drill

A coordinated cyber defense exercise designed to test and strengthen an organization's ability to prevent, detect, respond to, and recover from cyber threats.

In a Digital Shield drill, participants face simulated cyberattacks—such as phishing campaigns, ransomware outbreaks, data breaches, or network intrusions—in a controlled environment. The goal is to evaluate incident response plans, improve team coordination, identify security gaps, and enhance overall cyber resilience.

Such drills are commonly conducted by governments entities to ensure preparedness against real-world cyber threats. They help build awareness, improve technical skills, and strengthen cybersecurity frameworks across participating entities.

Digital Alert and SOAR workshop

Event Part 1: Security Orchestration, Automation, and Response (SOAR)

- Challenges in Security Operations
- The need for SOAR
- Introduction to FortiSOAR:
  - Overview of FortiSOAR platform
  - Key features and capabilities
  - Integration capabilities
  - Benefits of implementing FortiSOAR in security operations

Event Part 2: Digital Alert Platform

1. Why This Matters: Critical need for advanced threat protection.
2. The Story & Vision Journey, vision, partnership evolution.
3. Core Technology Components Key technologies powering the service 4
4. Real-World Use Cases: Government agency applications.
5. Onboarding & Next Steps: Integration & customer guidance.
6. The Road Ahead: Service roadmap and enhancements

Cyber Readiness Initiative

A scenario-based exercise that tests an organization's ability to respond to major cyber incidents. It will challenge participants to:

- Make critical decisions under pressure
- Coordinate across teams
- Manage the technical, operational, and reputational impacts of a simulated cyberattack

The simulation helps improve readiness, communication, and strategic response in real-world cyber crises

Events involvement

1. Intersec 2025 (UAE)
2. GPRC Summit (UAE)
3. Arab Health 2025 (UAE)
4. Dubai Airshow 2025 (UAE)
5. World Crisis & Emergency Management Summit 2025 (UAE)
6. Economy Middle East Summit 2025 (UAE)
7. World Government Summit 2025 (UAE)
8. CAISEC Conference (Egypt)
9. GITEX Asia 2025 (Singapore)
10. GITEX Africa 2025 (Morocco)
11. Japan Expo 2025 (Japan)
12. Cybertech Tokyo 2025 (Japan)
13. Billington Cyber Summit 2025 (Washington D.C., USA)
14. CIISec Live 2025 (United Kingdom)

15. Visit to the Maldives (Maldives)
16. Multilateral Cyber Financial Forum (Japan)
17. 4th meeting of the GCC Ministerial Committee on Cyber security Authorities and Centres (Kuwait)
18. 2nd regular session of the Arab Cyber security Ministers' Council (Kingdom of Saudi Arabia)
19. Black Hat MEA (Kingdom of Saudi Arabia)
20. EU-GCC Cyber security Roundtable (Kingdom of Saudi Arabia)
21. First Arab Cyber security Exercise 2025 (Qatar)
22. World Economic Forum Annual Meeting 2026 (Davos, Switzerland)

2026 PLANNED ACTIVITIES

In 2026, the UAE Cyber Security Council will continue advancing the initiatives established throughout the past years. Planned activities include hosting major national and international cyber security platforms such as GISEC and GITEX, organizing the next edition of CyberQ and leading the Global Cyber Drill in partnership with international stakeholders. Efforts across the Council's core pillars (policy development, operational readiness, awareness, leadership enablement) will be further strengthened, with a focus on sector-wide cyber exercises, international cooperation, strategic partnerships and capability-building programs. These activities will support the UAE's ongoing commitment to developing a secure, resilient and future-ready digital ecosystem.

CONCLUSION

The UAE Cyber Security Council continued to advance national cyber security priorities and strengthen the UAE's global presence in the field. The release of the National Cyber security Strategy 2025–2031 set a clear long-term vision for safeguarding the country's digital ecosystem, supported by ongoing policy updates and regulatory improvements.
Major global platforms such as GISEC 2025, GITEX 2025, CyberQ 2025 and the Meridian Conference offered opportunities for high-level dialogue, knowledge exchange and international engagement, helping shape future approaches to cyber governance. These efforts were complemented by sustained work across operational readiness and talent development, as well as international cooperation.

Looking ahead, CSC remains focused on expanding national capabilities and strengthening global partnerships, leading initiatives that reinforce the UAE's readiness and resilience in an increasingly complex cyber security landscape.

Guinness World Records received at GISEC 2025 for the Global CyberDrill

CSC presence on the Main Stage at GISEC 2025

Guinness World Records received at CyberQ 2025

Meridian Conference

CSC on the main stage of GITEX 2025

National Cyber Governance Summit 2025

CSC and ITU High-Level Meeting

CSC participation in the second ordinary session of the Arab Cybersecurity Ministers' Council, held in the Kingdom of Saudi Arabia.

Launch of the second cohort of the CyberE71 Incubator Programme at GITEX Dubai 2025

CSC participation at the EU-GCC Cyber Diplomacy 1.5 Dialogue in Riyadh

CSC hosting the UAE Cyber Governance Summit 2025 in Sharjah

CSC participating in the Billington Cybersecurity Summit 2025, held in Washington, D.C.

CSC participating in Cybertech Tokyo 2025

CSC delegation inaugurated the Cybersecurity Operations Centre in the Republic of the Maldives

CSC at the 4th GCC Ministerial Committee Meeting on Cybersecurity in Kuwait

UZBEKISTAN

UZCERT
(UZBEKISTAN COMPUTER EMERGENCY RESPONSE TEAM)

HIGHLIGHTS OF 2025

Summary of Major Activities

In 2025, UZCERT made major strides in strengthening Uzbekistan's cybersecurity by launching new initiatives and improving existing services to better protect its constituency and keep organizations informed about cyber threats. The team also took part in more than 20 international conferences and held workshops for government institutions, helping to boost the country's overall cyber readiness.

Achievements

- On October 6-7, 2025, the SUE "Cybersecurity center" and UZCERT team, in collaboration with the British company DIALOGUE, successfully organized the 3rd Cybersecurity Summit, Central Eurasia – CSS 2025 in Tashkent. The summit gathered around 60 companies from over 30 countries, with a total of more than 120 delegates in attendance.
- On February 26-27, 2026, the SUE "Cybersecurity center" and UZCERT team, in collaboration with the FIRST organization and INHA University in Tashkent, successfully organized the "FIRST Regional Symposium Central Asia - 2026" for the first time in Central Asia.

ABOUT ORGANIZATION

Uzbekistan Computer Emergency Response Team (UZCERT) stands as a divisional entity within the State Unitary Enterprise "Cybersecurity Center," dedicated to safeguarding Uzbekistan's cyber landscape. As a specialized service, UZCERT is dedicated to fostering collaboration and interaction with key stakeholders, including internet service providers, law enforcement agencies, and users across the national internet segment. Our core mission revolves around mitigating cyber risks, increasing cyebrsecurity awareness, providing timely and effective support in responding to cybersecurity incidents.

ACTIVITIES & OPERATION

Scope and definitions

The organization's activities encompass cybersecurity operations, threat monitoring, incident response, and advisory services within the Republic of Uzbekistan. Its constituency includes state and economic management bodies, local government entities, law enforcement agencies, critical information infrastructure (CII) operators, as well as legal entities and individuals. The scope extends to users, owners, and administrators of information systems and resources, ensuring comprehensive cybersecurity support across various sectors.

Abuse statistics

- UZCERT detected & analyzed over 2M cyber threats and vulnerabilities within Uzbekistan's national internet segment. UZCERT actively addressed these threats, providing notifications on threats & necessary recommendations and mitigation strategies to enhance cybersecurity resilience.
- Identified and shut down more than 159 phishing websites & malicious resources to prevent fraudulent activities.

New service(s)

During the 2025, existing services were significantly enhanced and further matured. The WAF as a Service, Early-Warning Service, and Advanced Honeypot Services underwent continuous development, improving detection accuracy, response capabilities, and overall effectiveness, ensuring stronger protection for government organizations against evolving cyber threats and strengthening national cybersecurity resilience.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- Conducted more than 10 training seminars for government agencies, organizations, and commercial bank employees.
- 2 international events were organized in collaboration with international partners.
- Organized "Blue Team" Competition at Cyberkent 3.0 (2025) International cybersecurity competition: Participants tested their skills in a simulated cyber attack-defense competition. Also, they developed practical skills in cybersecurity defense and threat mitigation.
- "Cybersecurity Summit, Central Eurasia – CSS 2025"
- "FIRST Regional Symposium Central Asia"

Events involvement

- UZCERT specialists have enhanced their skills in Digital Forensics, SOC operations, Threat Hunting, Red Team Operations, and Cyber Threat Monitoring & Response. They participated

in 13 online training seminars and 2 offline conferences organized Engagement in Cyber Competitions.

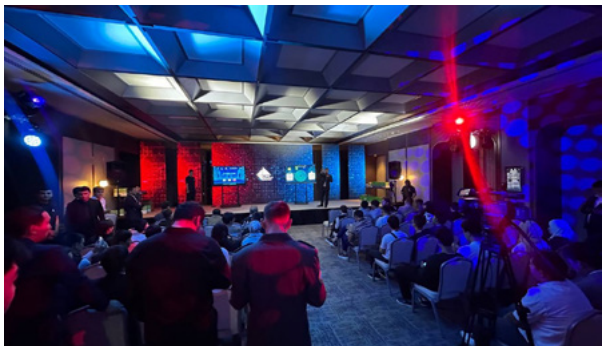
2026 PLANNED ACTIVITIES

- Hosting and organizing "Cyber Security Summit - Central Eurasia 2026";
- Organizing "CyberKent" (2026) national CTF competition;
- Expansion of the free national early-warning service to enhance cyber threat detection and response capabilities;
- Participation in regional and global cybersecurity conferences and summits to stay abreast of the latest developments in the field.
- Improvement of CSIRT activities (according to SIM3);

CONCLUSION

In 2025, UZCERT strengthened Uzbekistan's cybersecurity through enhanced services, proactive threat detection, and effective incident response. Over 2 million threats were analyzed, and malicious resources mitigated. International cooperation, major events, and capacity-building initiatives further improved national cyber resilience, positioning UZCERT as a key authority in protecting the country's digital infrastructure.

"Cybersecurity Summit, Central Eurasia – CSS 2025"



"FIRST Regional Symposium Central Asia - 2026"

COMMERCIAL MEMBERS

CERT-GIB

HIGHLIGHTS OF 2025

Summary of Major Activities

- Operation Secure, June 2025: In collaboration with INTERPOL, CERT-GIB provided mission-critical data on infostealer infrastructure (including Lumma and Risepro) in Asia. This input led to the arrest of 32 suspects and the takedown of over 20,000 malicious IPs and domains, protecting approximately 216,000 potential victims.
- Joint Operation (Thai/Singapore Police): In February 2025, Group-IB's investigations helped identify a prolific threat actor operating under aliases like ALTDOS and DESORDEN. By correlating digital personas across the dark web, CERT-GIB enabled the seizure of 13TB of stolen data and the arrest of a suspect responsible for over 90 global data leaks.
- BlackHat MEA: We made a powerful impact at Black Hat MEA 2025, proudly representing our brand at the region's largest cybersecurity gathering. We signed 6 new MoUs, celebrated key customer achievements, and saw nonstop engagement at our Cyber and Fraud Fusion Center booth, generating 430 high-quality leads. Our speaking sessions on deepfakes, fraud and emerging cyber risks reinforced our thought-leadership position, while strong PR activity with 9 interviews delivered wide media visibility across interviews and press announcements.
- Fraud Intel Pakistan, Karachi, 4th February: Group-IB hosted an exclusive BFSI-focused event in Pakistan, gathering Pakistan Regulator NCERT and 40 + C-level banking leaders to discuss the rapidly evolving fraud landscape.
- In Riyadh, Saudi Arabia, we had the privilege of hosting two exclusive Customer Advisory Board events, bringing together representatives from seven leading banks and 15 C-level executives for an evening of strategic discussions focused on identity security.
- CERT-GIB reported a 17% increase in the detection of both phishing and scam resources.
- CERT-GIB responded to more than 26,000 phishing resources and 118,000 scam resources, achieving successful takedowns of 99% of these.

Achievements

- Signed MOU with Pakistan CERT in Blackhat MEA in Riyadh, Saudi Arabia in December 2025
- Participated in 5 events with INTERPOL as speaker and added value on the cybersecurity sessions
- Launched Egypt Office in an stunning event with 300+ end clients and partners attendees from government, banking and critical sectors.

ABOUT ORGANIZATION

CERT-GIB (https://group-ib.com/) is the Computer Emergency Response Team created by the global cybersecurity company Group-IB. It is launched with the mission to immediately contain cyber threats, regardless of when, where they take place, and who is involved. CERT-GIB combines the power of human intelligence with technological prowess to offer the most effective response and remediation actions.

Group-IB adopted a decentralized operational strategy enabling collective action against cybercrime and comprehensive coverage of threat actors across all geographies for information exchange as the only effective long-term solution. Group-IB's GLOCAL strategy ensures the most robust response to cybercrime worldwide through its Digital Crime Resistance Centers (DCRCs), which deliver immediate, comprehensive, localized expertise and intelligence support. DCRC network spans multiple strategic locations, including Singapore, the Netherlands, UAE, Saudi Arabia, Vietnam, Malaysia, Thailand, Italy, Uzbekistan, Chile, and Egypt.

Group-IB introduced the Cyber Fusion Center (CFC) as an intelligence-driven evolution of the traditional SOC, designed to unify threat intelligence, hunting, and response into a single, proactive ecosystem. By fusing internal telemetry with external intelligence, the CFC moves beyond the reactive nature of a traditional SOC to anticipate and disrupt attacks during the adversary's reconnaissance phase.

Aside from being an OIC-CERT member, CERT-GIB is a member of Trusted Introducer, Anti-Phishing Working Group (APWG), FIRST, APCERT, Europol European Cybercrime Centre's (EC3) Advisory Group on Internet Security, and a strategic partner of Afripol and the International Multilateral Partnership Against Cyber Threats (IMPACT).

ACTIVITIES & OPERATION

Scope and definitions

CERT-GIB is a round-the-clock emergency response team that performs threat monitoring, helps contain threats, and brings trusted incident responders, forensic analysts, and investigation experts on the scene if needed, thereby eliminating costly delays.

Group-IB has provided more than 1,500 successful investigations and has spent over 70,000 hours responding to incidents of various complexity all over the globe. Group-IB has conducted extensive research on APT groups, ransomware operators, and general cybersecurity trends across all major industries. Group-IB's integration of advanced technological capabilities with human intelligence ensures that the company stays informed about the latest tools and tactics, techniques, and procedures (TTPs) employed by cybercriminals.

Incident handling reports

Operation Secure with INTERPOL

In early 2025, Group-IB played a pivotal role in Operation Secure, a major INTERPOL-led initiative that successfully dismantled infostealer infrastructure in Asia, protecting over 216,000 potential victims. The operation resulted in 32 arrests and the takedown of more than 20,000 malicious domains and IPs. Group-IB's High-Tech Crime Investigations and Threat Intelligence teams provided the mission-critical data that fueled the operation, specifically identifying compromised user accounts, analyzing the command-and-control (C2) infrastructure for malware like Lumma and Risepro, and tracking dark web and Telegram channels used to sell stolen data. By sharing this actionable intelligence with INTERPOL and local agencies in Vietnam, Sri Lanka, and Hong Kong, Group-IB enabled law enforcement to seize 41 servers and 100GB of criminal data, effectively disrupting the Malware-as-a-Service (MaaS) ecosystem.

Operation ALTDOS takedown with the Royal Thai Police and Singapore Police Force

In early 2025, Group-IB played a critical role in a joint operation with the Royal Thai Police and the Singapore Police Force that led to the arrest of a prolific cybercriminal responsible for over 90 data leaks worldwide, including 65 in the Asia-Pacific region. Operating under aliases such as ALTDOS, DESORDEN, GHOSTR, and 0mid16B, the individual exfiltrated more than 13TB of personal data and blackmailed victims by threatening to notify regulators and the media. Group-IB's High-Tech Crime Investigation and Threat Intelligence teams provided the essential breakthrough by using dark web monitoring technologies to correlate the cybercriminal's shifting digital personas, writing styles, and attack patterns across multiple years. By identifying the technical link between these aliases and tracking the individual's infrastructure—including the use of SQL injection tools and compromised RDP servers—Group-IB enabled law enforcement to execute raids that resulted in the seizure of electronic devices and luxury goods purchased with criminal proceeds.

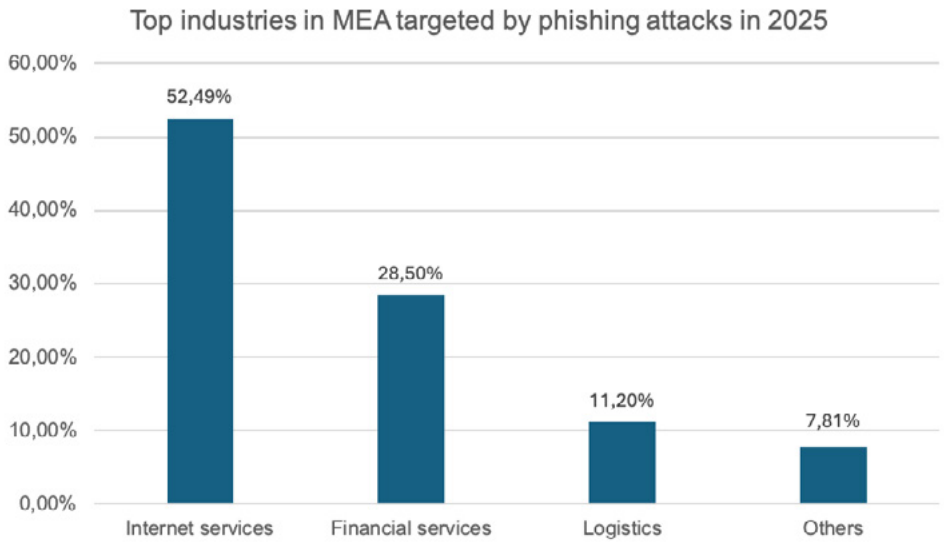
Abuse statistics

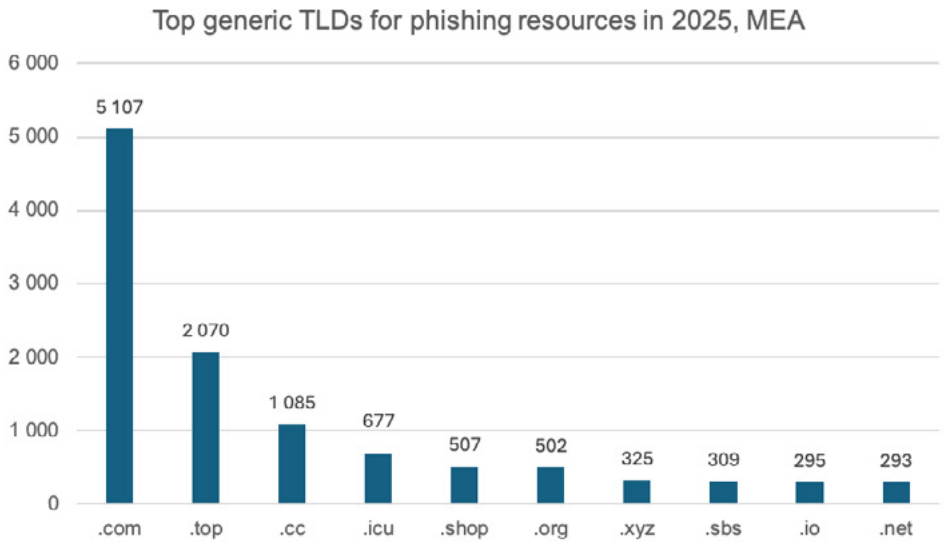
In 2025, CERT-GIB detected more than 96,000 phishing websites, marking a 17% increase over the previous year. In MEA, the most targeted industries were Internet services, financial services and logistics, accounting for 52.49%, 28.5%, and 11.2% of phishing websites, respectively.

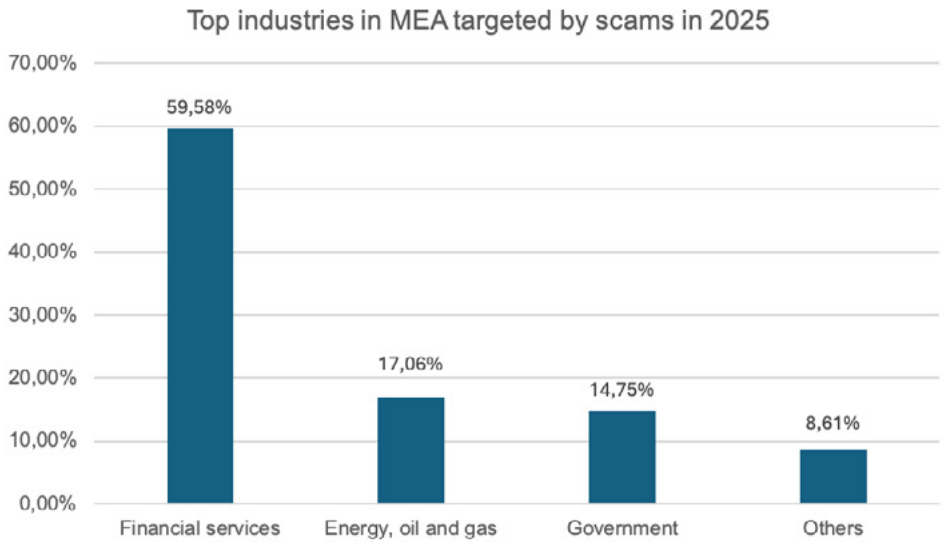
CERT-GIB also detected more than 150,000 scam resources, with nearly 60% of observed scams in MEA targeting the financial institutions.

One of the key responsibilities of CERT-GIB is not only to detect violations, but also to take down violating resources. CERT-GIB actively interacts with domain name registrars, TLD administrators, ISPs, as well as with other CERT and CSIRT teams to eliminate the violations.

In 2025, CERT-GIB responded to more than 26,000 phishing resources and 118,000 scam resources, achieving successful takedowns of 99% of these.


Top industries in MEA targeted by phishing attacks in 2025
60,00%
50,00%
40,00%
30,00%
20,00%
10,00%
0,00%
52,49%
28,50%
11,20%
7,81%
Internet services
Financial services
Logistics
Others


Top generic TLDs for phishing resources in 2025, MEA
6 000
5 000
4 000
3 000
2 000
1 000
0
5 107
2 070
1 085
677
507
502
325
309
295
293
.com
.top
.cc
.icu
.shop
.org
.xyz
.sbs
.io
.net


Top industries in MEA targeted by scams in 2025
70,00%
60,00%
50,00%
40,00%
30,00%
20,00%
10,00%
0,00%
59,58%
17,06%
14,75%
8,61%
Financial services
Energy, oil and gas
Government
Others

Publications

No	Publication	Link
1	Cyber Predictions For 2025 (and Beyond)	https://www.group-ib.com/blog/cyber-predictions-for-2025/
2	LATAM Intelligence Insights Report, January 2025	https://www.group-ib.com/resources/research-hub/latam-intelligence-insights-january-2025/
3	North America Intelligence Insights Report, January 2025	https://www.group-ib.com/resources/research-hub/north-america-intelligence-insights-january-2025/
4	APAC Intelligence Insights Report, January 2025	https://www.group-ib.com/resources/research-hub/apac-intelligence-insights-january-2025/
5	META Intelligence Insights Report, January 2025	https://www.group-ib.com/resources/research-hub/meta-intelligence-insights-january-2025/
6	Europe Intelligence Insights Report, January 2025	https://www.group-ib.com/resources/research-hub/europe-intelligence-insights-january-2025/
7	Emerging Risks of Card Testing Attacks: Rise of AI Agents	https://www.group-ib.com/blog/the-dark-side-of-automation-and-rise-of-ai-agent/
8	High-Tech Crime Trends Report 2025 (Annual Flagship)	https://www.group-ib.com/media-center/press-releases/high-tech-crime-trends-report-2025/
9	Joint Operation: Royal Thai and Singapore Police Force Arrest (ALTDOS)	https://www.group-ib.com/media-center/press-releases/joint-operation-with-royal-thai-police-and-singapore-police-force/
10	Europe Intelligence Insights Report, February 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-europe-february-2025/
11	APAC Intelligence Insights Report, February 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-apac-february-2025/
12	META Intelligence Insights Report, February 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-meta-february-2025/
13	The Cybercriminal with Four Faces: Unmasking DESORDEN/ALTDOS	https://www.group-ib.com/blog/the-cybercriminal-with-four-faces-revealing-group-ib-s-investigation-into-altdos-desorden-ghostr-and-0mid16b/
14	Europe Intelligence Insights Report, March 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-europe-march-2025/

No	Publication	Link
15	Intelligence Insights Report, March/April 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-march-april-2025/
16	Group-IB Earns 5-Star Rating in 2025 CRN® Partner Program Guide	https://www.group-ib.com/media-center/press-releases/5star-rating-crn-guide-2025/
17	Strategic MoUs at GISEC Global 2025: Launching Cyber Fusion Center	https://www.group-ib.com/media-center/press-releases/group-ib-signs-strategic-mous-with-local-and-regional-cybersecurity-leaders-at-gisec-global-2025/
18	Digital Risk Highlights 2025: Global Scam Tactics	https://www.group-ib.com/resources/research-hub/digital-risk-highlights-2025/
19	Intelligence Insights Report, May 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-may-2025/
20	Top 10 Masked Actors for 2025 (The Cybercrime Ranking)	https://www.group-ib.com/masked-actors/
21	Operation Secure: Group-IB Contributes to INTERPOL Infostealer Bust	https://www.group-ib.com/media-center/press-releases/interpol-infostealer-bust/
22	Intelligence Insights Report, June 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-june-2025/
23	Middle East Cyber Escalation: From Hacktivism to Threat Ops	https://www.group-ib.com/blog/middle-east-cyber-escalation/
24	Intelligence Insights Report, July 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-july-2025/
25	APAC Intelligence Insights Report, July 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-apac-july-2025/
26	META & Pakistan Intelligence Insights Report, July 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-meta-july-2025/
27	Intelligence Insights Report, August 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-august-2025/
28	META Intelligence Report, August 2025	https://www.group-ib.com/resources/research-hub/meta-intelligence-report-august-2025/
29	APAC Digital Risk Protection Cases Report, August 2025	https://www.group-ib.com/resources/research-hub/apac-digital-risk-protection-cases-report-august-2025/

No	Publication	Link
30	Operation Serengeti 2.0: INTERPOL Africa Infrastructure Takedowns	https://www.group-ib.com/media-center/press-releases/operation-serengeti-2-0/
31	Hacktivist at War: The Cambodia-Thailand Cyber Escalation	https://www.group-ib.com/resources/research-hub/cambodia-thailand-cyber-escalation-2025/
32	From Deepfakes to Dark LLMs: 5 Use-cases of AI in Cybercrime	https://www.group-ib.com/blog/ai-cybercrime-usecases/
33	Europe Intelligence Insights, September 2025	https://www.group-ib.com/resources/research-hub/europe-intelligence-insights-september-2025/
34	Operation Contender 3.0: Group-IB Intelligence Leads to 260 Arrests	https://www.group-ib.com/media-center/press-releases/operation-contender3/
35	A New Weapon Against Payment Fraud: Suspicious Payment Details	https://www.group-ib.com/blog/payment-fraud-defense/
36	Unmasking MuddyWater's New Malware Toolkit (International Espionage)	https://www.group-ib.com/blog/muddywater-espionage/
37	Europe Intelligence Insights, October 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-europe-october-2025/
38	Intelligence Insights Report, October 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-october-2025/
39	Uncovering a Multi-Stage Phishing Kit Targeting Italy's Infrastructure	https://www.group-ib.com/blog/uncover-phishing-italy/
40	Bloody Wolf: A Blunt Crowbar Threat To Justice (Central Asia)	https://www.group-ib.com/blog/bloody-wolf-threat/
41	AUNZ Intelligence Insights, November 2025	https://www.group-ib.com/resources/research-hub/aunz-intelligence-insights-november-2025/
42	Intelligence Insights Report, November 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-november-2025/
43	Choose Your Fighter: Evolution of Android SMS Stealers in Uzbekistan	https://www.group-ib.com/blog/mobile-malware-uzbekistan/
44	Intelligence Insights Report, December 2025	https://www.group-ib.com/resources/research-hub/intelligence-insights-december-2025/
45	White Paper: CYBERSECURITY X AI (eGuide)	https://www.group-ib.com/resources/white-papers/cybersecurity-ai-capabilities/

No	Publication	Link
46	White Paper: Weaponized AI: Inside The Criminal Ecosystem	https://www.group-ib.com/resources/white-papers/weaponized-ai-criminal-ecosystem/

New services

1. Cyber Fraud Intelligence Platform (CFIP)
Launched in December 2025, the CFIP is arguably the most significant product addition of the year. It is a real-time, GDPR-compliant solution that allows banks and financial institutions to collaborate and share "suspicious" risk signals (not just confirmed fraud) without compromising user privacy.

2. AI Assistant
Introduced at GISEC Global 2025, this AI-powered tool was integrated across the Group-IB ecosystem to streamline how analysts interact with complex data. It allows security professionals to use plain-language queries to extract structured, context-rich insights from the Threat Intelligence and Digital Risk Protection modules.

3. Enhanced "Cyber Fusion Center" (CFC) Ecosystem
While the CFC is a core Group-IB concept, 2025 saw its full realization as a "unified ecosystem" showcased at major events. It now formally unifies Fraud Protection, Threat Intelligence, DRP, and MXDR into a single workflow.

4. New Global Partner Programme
Launched in April 2025, this was a major service-expansion initiative aimed at resellers and MSSPs.

Structure: A five-tier system (Standard to Platinum) that gives partners early access to product features and collaborative marketing.

Partner Academy: A new educational service offering specialized certifications to help partners address the complex threats identified in Group-IB's 2025 research.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

No.	Event	Date
1	Partner Universe META	27th February 2025
2	Al Shafak Event for Libyan Customers	11th April 2025
3	Partner Connect KSA	12th May 2025
4	Brunei Cybersecurity Association Visit (Kuala Lumpur)	20th May 2025
5	Egypt Office Opening Event	24th May 2025

No.	Event	Date
6	D360 Bank ABM Event (Riyadh)	15th July 2025
7	KSA Fintech Event - Committee SAMA	3rd September 2025
8	Customer Advisory Board Meeting (Riyadh)	27th October 2025
9	Royal Malaysia Police Force (PDRM) Workshop	28th October 2025
10	Turkey Banking Roundtable Event	4th November 2025
11	Malaysia Ministry of Defence (MINDEF) Technology Workshop	5th November 2025
12	UBF Banking Roundtable (UAE)	26th November 2025

Events involvement

No	Event	Date
1	Cyber First Kuwait	21st April 2025
2	GISEC Global (Dubai)	6th – 8th May 2025
3	CAISEC (Egypt)	25th – 27th May 2025
4	IAFPC	19th June 2025
5	InfoSec Karachi	24th July 2025
6	E-Crime Congress Abu Dhabi	10th September 2025
7	IDC Security Summit Turkey	25th September 2025
8	DSI Forum Tunisia	29th – 30th October 2025
9	AICS Bahrain Event	4th November 2025
10	IDC CISO Roundtable KSA	10th November 2025
11	CTI Islamabad	13th November 2025
12	Cairo ICT (Egypt)	16th – 18th November 2025
13	C8 Jordan Event	18th – 20th November 2025
14	Customer Advisory Board KSA (HTCT Focus)	19th November 2025
15	Black Hat KSA (MEA)	2nd – 4th December 2025
16	Fraud Intel Pakistan	4th February 2026
17	MCC Event Tunisia	11th – 12th February 2026

2026 PLANNED ACTIVITIES

No.	Event	Date
1	3rd Party Event South Africa - Capetown	January
2	Partner Connect - Eastern KSA	January
3	MCC Conference Tunisia	January
4	Ramadan Suhoor Jordan	February
5	Nullcon Goa	February
6	ABM Fraud Intel Pakistan	March
7	Partner Universe META	April
8	ENBANTEC Turkey	April
9	Al Shafak Customer Event	April
10	Oman data park Customer Event	April
11	IAFPC 3.0 Dubai, UAE	April
12	ABM Event Bahrain	April
13	Saudi Office Opening Event	April
14	GISEC	May
15	Office Event for NAEL customers in Sharm El Shiekh	May
16	Customer Advisory Board UAE	May
17	CAISEC Egypt	May
18	Fraud Intel Egypt	May
19	Business Breakfast - Jeddah	May
20	AWS Launch Event KSA	May
21	Lunch & Learn Partner Event	May
22	IDC IT Security Summit Saudi Arabia	June
23	Customer Advisory Board Egypt	July
24	Partner Connect Turkey	July
25	Pakistan GOV accounts partner led event (Premier partner)	July
26	Infosec Pakistan	July
27	3rd Party Event South Africa - Johannesburg	July
28	Malaysia NACSA Cybersecurity Summit (CYDES)	July
29	Malaysia Fintech Summit	July
30	Fraud Intel Jordan	August
31	Lunch & Learn Partner Event	August
32	Fraud Day Bahrain with GBM	August

No.	Event	Date
33	ABM Business Breakfast - Dammam	August
34	Blackhat Space Payment	August
35	ABM ENBANTEC BFSI Roundtable - Turkey	August
36	Libya Tech Forum	September
37	E-crime Congress UAE	September
38	Pakistan Cyber Crime Summit	September
39	IDC Security Summit - Turkey	September
40	CPX Customer Roundtable UAE	October
41	Business Breakfast - Kenya	October
42	Ghana/Nigeria Event	October
43	ABM South Africa Launch Event	October
44	ABM Kuwait Roundtable Event	October
45	Partner Event - Egypt	October
46	CAIRO ICT	October
47	Partner Connect KSA	October
48	Cybercrime Summit KSA	October
49	C8 Jordan	October
50	Lunch & Learn Partner Event UAE	October
51	Customer Advisory Board KSA	October
52	Morocco Customer Roundtable	October
53	CTI Karachi	November
54	Blackhat MEA	December

CONCLUSION

In 2025, CERT-GIB maintained a significant and proactive presence in global anti-phishing and anti-scam initiatives, which were instrumental in safeguarding individuals and organizations across the digital landscape. The team recorded a 17% increase in the detection of phishing and scam resources, identifying more than 96,000 phishing websites and 150,000 scam resources throughout the year. This rigorous monitoring, combined with active collaboration with ISPs and registrars, allowed CERT-GIB to achieve a successful takedown rate of 99% for handled violations, providing critical protection to highly targeted sectors such as financial services and logistics.

Strategic collaboration with international law enforcement remained a cornerstone of Group-IB's mission, as evidenced by its role in major actions such as Operation Secure and the ALTDOS infrastructure takedown. By providing mission-critical intelligence and correlating complex digital

personas, the team directly contributed to the arrest of numerous cybercriminals and the seizure of massive amounts of stolen data. These operational successes, supported by over 70,000 hours of incident response and more than 1,500 successful investigations, have allowed Group-IB to refine its strategies and share vital knowledge regarding the latest tactics, techniques, and procedures (TTPs) with the global cybersecurity community.

As the future is approached, Group-IB is expected to continue this momentum. In the coming year, capabilities will be enhanced by leveraging advanced artificial intelligence technologies, enabling the organization to stay ahead of evolving threats and further bolster defenses. The commitment to innovation and expertise sharing will remain at the forefront of the mission, ensuring that partners, clients, and the global community are protected and a safer digital environment for all is contributed too.

Exchange of MOU signing Group-IB and National CERT – Pakistan.

Fraud Intel Pakistan Event Panel Discussion on the topic Cyber Fraud in Pakistan:From Engineering to Organized Crime

Picture with clients and Group-IB team at the Customer Advisory Board 2.0 Meeting.

Saudi National Bank (SNB) awarded the Excellence in Cyber Fraud award in Black Hat MEA 2025

Group-IB Team Picture in Egypt Office Opening Event Cairo, Egypt

CTM360

Summary of Major Activities

Over the course of the year, CTM360 drove continuous technological innovation, strengthened its global presence, and actively contributed to global cybersecurity initiatives.

Key highlights included:

- Enhanced Digital Risk Protection platform with advanced modules and features to address the evolving threat landscape, leveraging AI and automation, threat intelligence, and scalable monitoring capabilities.
- Mapped and profiled threat data in terms of the digital assets for 1.39+ million organizations worldwide.
- Expanded global presence with a new office in Malaysia, which will serve as a regional hub for partners across Southeast Asia.
- Engaged in strategic partnerships with regulators, national cybersecurity agencies, and telecommunication authorities to strengthen national cybersecurity posture across multiple regions.
- Hosted high-level roundtables and closed-door knowledge-sharing sessions across various countries, bringing together policymakers and corporate leaders to address emerging digital risks and fraud.
- Supported the ongoing ITU Cyber for Good program to enhance cyber resilience and bridge the cybersecurity gap in Least Developed Countries (LDCs) and Small Island Developing States (SIDS). Read More https://www.itu.int/partner2connect/flash-edition-10/

Achievements

Capacity-Building Initiatives:
CTM360 continued to enhance its global capacity-building initiatives by providing support to over 55 national CERTs through its consolidated Digital Risk Protection platform. These initiatives strengthened national-level threat monitoring, improved risk visibility, and enhanced cyber resilience across multiple regions.

Global Customer Expansion:
Global Customer Base: CTM360 continued to scale its global presence, now serving over 2,000 customers across more than 100 countries. The company serves a diverse portfolio of clients across both public and private sectors, with a strong presence in key industries including banking and financial services, telecommunications, government, energy, aviation, and healthcare.

Community Edition: Alongside its commercial growth, CTM360 remains committed to advancing industry-wide cyber readiness through its free Community Edition Platform, which has now enabled over 1,200 organizations globally. This initiative empowers small and medium-sized enterprises (SMEs) with accessible tools to monitor and manage their cybersecurity posture without commercial barriers.

Memorandums of Understanding (MoUs):
CTM360 expanded formal partnerships with the following regulatory and cybersecurity authorities, establishing collaborative working relationships to enhance cybersecurity resilience across their respective CNIs.

- The Gambia Public Utilities Regulatory Authority (PURA)
  https://pura.gm/press-release-ctm360-partners-with-pura-to-strengthen-the-gambias-national-cybersecurity-resilience/
- Lesotho Communications Authority (LCA)
  https://www.thereporter.co.ls/2025/08/20/lca-signs-mou-to-strengthen-cybersecurity-infrastructure/
- ISACA Singapore Chapter
  https://ciosea.economictimes.indiatimes.com/news/security/ctm360-and-isaca-singapore-chapter-sign-mou-for-cybersecurity-collaboration/117503329

These partnerships focus on strengthening national cyber resilience, enhancing regulatory visibility, and supporting coordinated cyber defense initiatives.

Global Partnerships & Collaboration:
CTM360 continued to strengthen its global ecosystem through key strategic partnerships:

- In Saudi Arabia, CTM360 collaborated with Cyberani (Aramco Digital) to deliver its cybersecurity solutions through managed security services, extending advanced protection capabilities to enterprise customers.

  Read the press release here https://techafricanews.com/2026/01/05/cyberani-partners-with-ctm360-to-enhance-managed-cybersecurity-services-in-saudi-arabia/
- In Iraq, CTM360 joined forces with Cihan Bank to enhance digital brand protection and enable proactive threat monitoring across the financial sector.

  Read the press release here https://www.zawya.com/en/press-release/companies-news/cihan-bank-collaborates-with-ctm360-to-strengthen-its-brand-and-digital-risk-protection-in-iraq-kmygavnz
- In Egypt, CTM360 worked alongside Fawry, a leading fintech platform, to strengthen digital risk protection and deliver a more secure online experience for its customers and partners.

  Read the press release here: https://www.zawya.com/en/press-release/companies-news/fawry-joins-forces-with-ctm360-to-strengthen-digital-risk-protection-and-safeguard-customers-from-evolving-cyber-threats-s5xif5en

These collaborations enhanced cross-border coordination and collective efforts to counter fraud, brand abuse, and evolving cyber threats.

Establishing a Regional Office in Southeast Asia

Additionally, CTM360 expanded its presence in Southeast Asia with the launch of a regional hub in Kuala Lumpur, Malaysia. This on-the-ground presence enables CTM360 to deliver faster, more responsive support to public- and private-sector organizations by leveraging local insights and a deep understanding of the regional threat landscape. Through this expansion, the company seeks to strengthen collaboration with partners while providing advanced cybersecurity solutions tailored to the region's unique challenges and needs.

Read the press release here: https://www.zawya.com/en/press-release/companies-news/ctm360-announces-strategic-expansion-with-new-regional-hub-in-malaysia-m94ob8xa

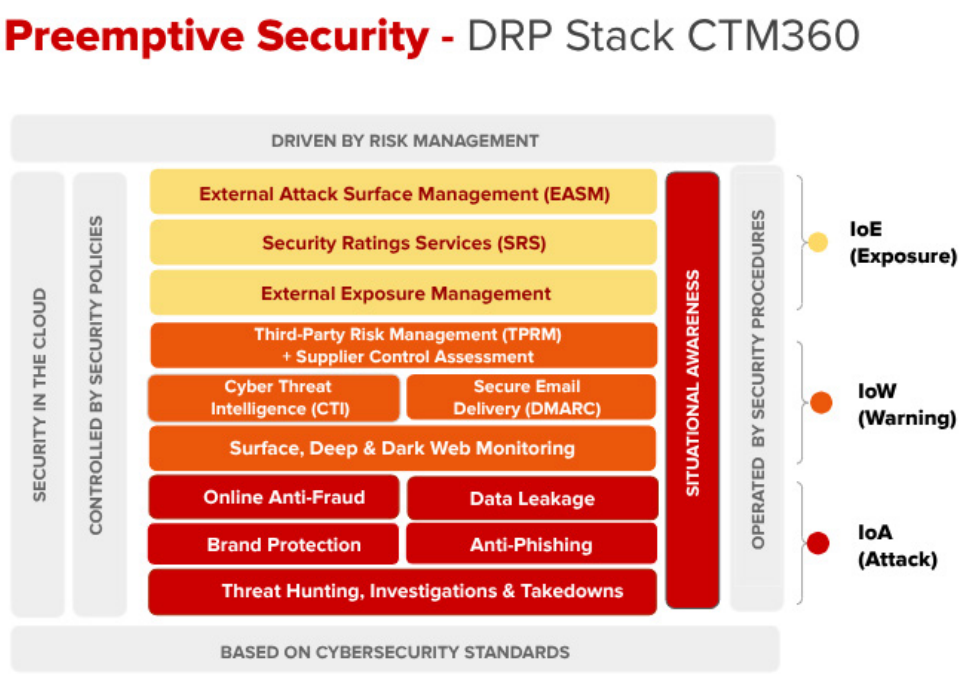
Launch of New Features in The DRP Stack

CTM360 introduced a range of new capabilities, features, and modules across its platform, including the Takedown and Reporting modules, as well as the Money Mule Account module. The Takedown module enables users to track the progress and timelines of takedown activities, while the Reporting module allows users to generate customized reports with board-level risk visibility. The platform was further enhanced with features such as the Ask AI chatbot and AI-driven threat detection. In addition, CTM360 launched 'CyNA', a cyber situational awareness app, and expanded the CTM360 Academy with new courses aligned to the latest modules.

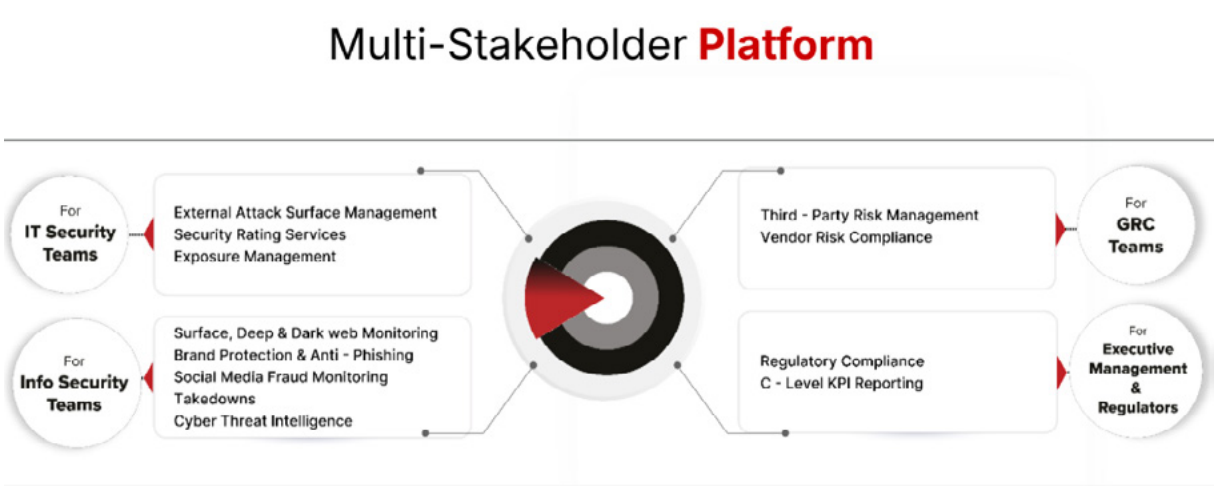
ABOUT ORGANIZATION

CTM360 was established in 2014 in the Kingdom of Bahrain as a technology company from the Arab world, driven by the vision "Cybersecurity from Bahrain to the World." As a pioneer in Offensive Defense and threat intelligence beyond the perimeter, the company invested heavily in building a consolidated technology platform to support its mission.

The platform delivers a fully managed, subscription-based cybersecurity technology that enables organizations to proactively identify, monitor, assess, and mitigate cyber risks and threats beyond the traditional network perimeter. Built on a preemptive cybersecurity model, the CTM360 DRP stack delivers actionable intelligence through its comprehensive Indicators of Exposure (IoE), Indicators of Warning (IoW), and Indicators of Attack (IoA). These early indicators empower organizations to shift from reactive to proactive defense, enabling them to mitigate risks and disrupt threats early in the attack lifecycle (Reconnaissance phase).



CTM360 is designed as a multi-stakeholder platform, delivering value to IT Security, Information Security, GRC, and Executive/Board-level stakeholders, each with tailored stats and insights aligned with their responsibilities.



The technology platform empowers governments, regulators, enterprises, financial institutions, and SMEs to proactively manage digital risks and threats while supporting data-driven security decisions.

As of 2025, CTM360 continues to advance its cybersecurity technology model, integrating artificial intelligence at the core of its platform to enhance threat detection, speed, precision, and predictive accuracy.

ACTIVITIES & OPERATION

Scope and definitions

The CTM360 platform operates at scale, ingesting billions of data points to enable global visibility into cyber risks and threats.

In addition to its global-scale monitoring capabilities, the CTM360 platform integrates advanced threat intelligence feeds, AI-driven detection capabilities, and coordinated response operations to deliver comprehensive end-to-end external threat management. The platform provides continuous monitoring across diverse digital environments and enables rapid threat disruption through structured validation processes and coordinated takedown workflows. Some operational statistics from 2025 include:

- CTM360 platform mapped and profiled 1.39 million organizations across the globe.
- Tracking and monitoring more than 42,000 threat actor claims across the globe.
- Extensively tracking the digital frauds, scams, and threats landscape across known and emerging use cases.

Incident handling reports

CTM360 operates one of the world's largest dedicated platforms for detecting and executing automated takedowns of digital fraud and scams, enabling rapid identification and response to emerging threats.

In 2025, CTM360 leveraged its WebHunt platform to process over 250+ million URLs, identifying approximately 4.5 million confirmed incidents across institutions worldwide. From this large-scale intelligence, incidents were validated and mapped to relevant organizations.

As a result, CTM360 detected and managed approximately 580,500+ incidents specific to its monitored members across digital fraud, scams, phishing, and their variants, while successfully resolving 356,400 incidents.

Abuse statistics

The CTM360 platform categorizes detected abuse incidents into multiple threat types, providing a comprehensive view of the evolving cyber risk landscape. In 2025, the WebHunt platform processed over 250+ million URLs, identifying millions of fraud, scams, and abuse-related instances across the global digital ecosystem.

This large-scale visibility enabled CTM360 to analyze abuse trends, identify emerging threat patterns, and understand the distribution of fraud activities across regions, industries, and attack types, supporting more effective detection and response operations.

Publication(s)

Research, Reports & Cyber Advisories:
CTM360 continued to publish a series of strategic research reports, threat analyses, and cyber advisories designed to help organizations proactively anticipate and mitigate evolving cyber fraud.

Read more about CTM360 Reports & Threat Insights Here:
https://www.ctm360.com/cybersecurity-reports

Published Reports (2025):

- HackOnChat: (The WhatsApp Hacking Scam Explained)
- Postal Courier Con: (Inside the World's Largest Postal & Courier Scam Campaigns)
- Scam Hooks: (How Even Smart People Take the Bait)
- FraudOnTok: (The SparkKitty Drop on TikTok Shops)
- BaitTrap: (The Rise of Baiting News Sites)
- Info-Stealers Malware Report: (Understanding the Silent Data Threat)
- Don't Be the Next Headline: (How to Harden Against Ransomware)
- CyberHelist Phish Report: (Simulating a Full Corporate Banking Breach)
- Meta Mirage Report: (Inside a Global Meta Phishing Operation)
- PointyPhish & TollShark Report: (Exposing the Global Phishing & Fraud Network)
- Play Masquerading Party (PMP) Report: (Unveiling the Global Play Store Impersonation)
- PlayPraetor Trojan Report: (Global Android Malware Campaign)

Published Reports (2026)

- ShadowRemit (Malicious Google Play Apps used for illegal money transfer)
- FraudWear (Inside the Cyber Threat of Brand-Impersonating Online Stores)
- The Rise of Fake Banks in the USA & UK (Analysis by CTM360)
- HYIPRisk (High Yield Investment Platforms: High Hopes, Higher Losses)
- Ninja Browser & Lumma Infostealer (Delivered via Weaponized Google Services)

New service(s)

Technology Expansion & Platform Enhancements:
CTM360 further upgraded its Digital Risk Protection (DRP) platform. New modules and enhanced platform capabilities were introduced to improve large-scale threat detection and accelerate takedown operations.

New Platform Modules:

Takedown Insights Module
CTM360 introduced Takedown Insights, a new module within CTM360's CyberBlindspot platform that provides a centralized view of all takedown activities. It enables organizations to monitor progress, measure success rates, and assess the overall impact of mitigation efforts.

Reporting Module
The new Reporting Module allows users to generate customized, data-driven reports with key insights from across the platform, simplifying executive communication and operational analysis.

Money Mule Account Module
CTM360 launched the Money Mule module, designed to give you enhanced visibility into suspicious money mule accounts linked to your organization.

CyNA Application:
CTM360 launched the CyNA (Cyber News, Alerts, and Advisories) App as a new cyber situational awareness module. Available on mobile, it provides curated threat intelligence, real-time alerts, and practical advisories to help organizations stay aware of emerging cyber risks and respond quickly.

New Platform Features

Ask AI
CTM360 launched Ask AI, an interactive feature embedded throughout the platform. It enables users to engage directly with the threat intelligence database, making it easier to retrieve insights and analyze information.

AI-Based Threat Detection
CTM360 enhanced the platform with advanced AI-driven threat detection capabilities designed to identify emerging cyber risks across the external digital landscape.

CTM360 Academy
CTM360 introduced the DeepScan Module Course as part of its Academy program. The course provides hands-on training on the DeepScan module, with a focus on advanced scanning methodologies and vulnerability validation across the underlying technology stack.

Fraud Navigator
CTM360 introduced the unique concept of Fraud Navigator, inspired by the MITRE framework. It is an analysis of the observed fraud, showing how scammers navigate through different stages of the fraud.

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization/agency

CTM360 Roundtable 2025- Azerbaijan

CTM360 Iftar Roundtable 2025 - Indonesia

CTM360 Roundtable 2025 - Jakarta

CTM360 Roundtable 2025 - Malaysia

CTM360 Burkapusa Iftar Roundtable 2025 - Malaysia

CTM360 Roundtable 2025 - Nigeria

CTM360 Roundtable 2025 - Sri Lanka

CTM360 Roundtable 2025 - Manila

CTM360 Roundtable 2025 - Nepal

Events involvement

37th ANNUAL FIRST CONFERENCE 2025

Arab International Cybersecurity Conference & Exhibition- AICS 2025

The National Cybersecurity Conference (NCSC) 2025 - Nigeria

RSA Conference 2025 - San Francisco

CGD Conference 2025 - Cherating, Malaysia

2026 PLANNED ACTIVITIES

As part of its 2026 engagement roadmap, CTM360 has already completed participation in several key industry initiatives, including:

1. FIRST Regional Symposium for Central Asia 2026 in Uzbekistan

2. Cyber Security Awareness Event organized by Crystal Tech Africa & CTM360

3. A partnership with NiceNIC (Hong Kong) to foster a safe and secure internet ecosystem.
Read the press release here:
https://nicenic.com/news/NiceNIC-Partners-with-ChainPatrol-and-CTM-to-Foster-a-Safe-and-Secure-Internet-Ecosystem-41846

CTM360 has outlined a series of strategic initiatives to further accelerate its growth and enhance platform capabilities in 2026. Key engagements include:

- Participation in the FIRST 2026 Cyber Threat Intelligence Conference as a Platinum Sponsor, reinforcing CTM360's leadership in global threat intelligence.

- Participation in the 38th Annual FIRST Conference in Denver, USA, as a Bronze Sponsor, strengthening engagement with the global cybersecurity community.
- Executive roundtable conferences across Sri Lanka, Indonesia, and Malaysia to drive regional dialogue and collaboration on cybersecurity challenges.
- Geographic expansion across Europe, North America, and Central Asia, supporting broader market penetration and customer acquisition.
- Signing of MoUs with national-level CERTs and regulatory bodies, including:
  - Cyber Defense Africa (CDA), Togo
  - Uganda Communications Commission
  - Malawi CERT
  - Ministry of Posts and Telecommunications (MOPT), Liberia
  - Information Network Security Administration (INSA), Ethiopia

Technology Enhancements (2026):

In 2026, CTM360 is set to introduce significant enhancements to its Digital Risk Protection (DRP) platform, focused on advancing automation, intelligence, and user experience:

- **AI-Driven Phishing Analysis & Enrichment (CyberBlindspot platform):**

  AI agents will analyze phishing pages to understand scam context and identify targeted data, delivering enriched intelligence to support both security analysts and automated response systems.
- **AI-Powered Incident Curation (CyberBlindspot platform):**

  CTM360 will deploy AI agents to streamline cyber incident analysis and intelligence enrichment. These capabilities will support threat classification, data enrichment, and structured intelligence generation.
- **AI-Based Asset Labeling (HackerView platform):**

  AI will automatically analyze discovered digital assets and generate contextual labels, enhancing risk prioritization and improving overall security analysis.
- **Platform Enhancements (RiskHub platform):**

  RiskHub will be enhanced to elevate the vendor risk management experience, with improvements in user interface, navigation, and visibility into vendor cyber risk exposure.

In addition, CTM360 aims to map and profile risk and threat intelligence for over 3 million organizations globally, further strengthening its data-driven cybersecurity capabilities.

CONCLUSION

As digital threats continue to evolve in scale and sophistication, particularly with the growing use of advanced AI in fraud campaigns, CTM360 continues to play an active role in addressing this new generation of risks. With adversaries increasingly leveraging automation and evasive techniques, the company anticipates a sustained rise in both the volume and complexity of cyber threats. In response, CTM360 is advancing its platform capabilities through enhanced automation and AI-driven detection, enabling more timely and accurate identification and mitigation of complex attack patterns. These efforts also contribute to broader ecosystem development, supporting initiatives such as incubators, accelerators, and research hubs that strengthen local expertise and digital resilience.

CTM360 has further expanded its contribution to national-level cybersecurity capacity through strategic collaborations with global institutions. These partnerships have extended support from Least Developed Countries to Small Island Developing States, reinforcing cyber resilience across diverse regions and contributing to scalable capacity-building models.

At the same time, CTM360 continues to expand its global footprint, strengthen its technical capabilities, and deepen its strategic alliances. Through its ongoing transition toward a product-led growth (PLG) model, the company is enhancing platform accessibility, enabling greater self-service capabilities, and delivering more scalable, data-driven value to organizations worldwide.

CTM360 remains committed to advancing cybersecurity through continuous innovation, actionable threat intelligence, and the proactive disruption of malicious activity. Through sustained collaboration and the continued expansion of its global ecosystem, the company contributes to building a more secure, resilient, and self-reliant digital future, while bringing technologies developed in the Arab world to a broader global audience.

TURKISH AIRLINES - COMPUTER EMERGENCY RESPONSE TEAM

HIGHLIGHTS OF 2025

- Achieved continuous monitoring and analysis of security events, ensuring timely identification and response to potential threats.
- Improved incident response efficiency through process optimization and enhanced alert handling mechanisms.
- Reduced alert noise and improved prioritization, enabling faster identification of critical security incidents.
- Strengthened threat detection capabilities by refining detection logic and monitoring strategies.
- Enhanced security visibility across systems to support more comprehensive threat analysis.
- Standardized security operations processes to improve consistency and operational effectiveness.
- Ensured effective coordination with internal stakeholders during security investigations and response activities.
- Maintained a resilient and continuous security operations capability throughout the year.

ABOUT ORGANIZATION

With more than 30 years of operational experience in the aviation industry, the organization integrates its extensive domain expertise with advanced technologies, including artificial intelligence, big data, cybersecurity, and fintech.

By leveraging its accumulated knowledge and technical capabilities, the organization develops innovative software solutions that support both industry-specific needs and broader digital transformation initiatives. These efforts contribute to enhancing operational efficiency, strengthening cybersecurity resilience, and shaping the future of global technology ecosystems.

ACTIVITIES & OPERATION

Security Monitoring and Incident Handling

Throughout the year, continuous monitoring of security alerts and potential cyber incidents was conducted. Detected events were analyzed and investigated to determine their impact and ensure appropriate response actions.

Security Operations Process Optimization
During the reporting period, improvements were made to internal security operations processes in order to enhance alert management efficiency and streamline incident handling procedures.

Enhancement of Threat Detection Capabilities
Existing monitoring and detection mechanisms were reviewed and refined to improve the identification of suspicious activities and potential cyber threats within the infrastructure.

Cyber Threat Landscape Monitoring
Ongoing monitoring of emerging cyber threats and attack techniques was performed to maintain situational awareness and support proactive defensive measures.

Operational Security Coordination
The team provided operational support and coordination with relevant internal units during security investigations and response activities.

Security Alert Prioritization Improvements
Alert prioritization mechanisms were improved to reduce operational noise and ensure faster identification of critical security events.

Security Visibility Improvement
Efforts were made to improve visibility into security events across monitored systems to support more effective threat detection and response.

Continuous Security Operations Support
Security monitoring activities were maintained on a continuous basis to support organizational cybersecurity resilience.

2026 PLANNED ACTIVITIES

Proactive Threat Hunting Capability Development
In 2026, the team plans to establish a structured threat hunting capability to proactively identify hidden threats within the environment. This includes defining threat hunting methodologies, use-case development, and integration with existing monitoring systems.

Development of Threat Hunting Use Cases and Playbooks
The team aims to develop and operationalize threat hunting scenarios based on real-world attack techniques and internal risk assessments. Standardized playbooks will be created to ensure consistency and repeatability of hunting activities.

Purple Teaming Activities
Planned activities include the introduction of purple teaming exercises to enhance collaboration between detection and response functions. These exercises will focus on validating detection capabilities and improving defensive mechanisms against advanced attack scenarios.

Enhancement of Detection Engineering Practices
Efforts will be made to further improve detection logic and correlation rules by leveraging insights gained from threat hunting and purple team exercises. This will support more effective identification of sophisticated threats.

Continuous Improvement of Incident Response Processes
Incident response processes will be further refined based on lessons learned from past incidents and proactive security activities, ensuring faster and more efficient response capabilities.

Expansion of Security Visibility and Data Sources
The team plans to expand visibility across the environment by integrating additional log sources and improving telemetry coverage to support advanced threat detection and analysis.

Strengthening Threat Intelligence Integration

Threat intelligence utilization will be enhanced to support both proactive threat hunting and real-time detection, ensuring better alignment with current threat landscape.

CONCLUSION

Throughout 2025, the organization continued to strengthen its cybersecurity operations by focusing on continuous monitoring, incident response, and operational process optimization. Key improvements in alert management, detection capabilities, and security visibility have contributed to a more efficient and responsive security operations environment.

In 2026, the organization aims to evolve from a reactive security model to a proactive and intelligence-led approach. The introduction of structured threat hunting practices, purple teaming activities, and enhanced detection engineering capabilities will play a critical role in identifying sophisticated threats and improving defensive readiness.

This strategic direction reflects a commitment to increasing the maturity of cybersecurity operations and building a more resilient and forward-looking security posture.

TURKCELL CYBER DEFENCE CENTER

HIGHLIGHTS OF 2025

Summary of Major Activities

In 2025, Turkcell CDC continued to offer new cyber security services for its corporate and individual customers:

Turkcell Security Operations Center (SOC) Service
As Turkcell Security Operations Center (SOC), we provide 24/7 continuous monitoring and incident response services in line with our mission to contribute to national cyber security and our vision to enhance organizational cyber resilience. We primarily serve large-scale enterprises with critical infrastructures, delivering end-to-end security operations management across various sectors. By adopting a proactive approach against the evolving threat landscape, we aim not only to detect incidents but also to enable early warning and preventive measures to continuously improve our customers' security maturity.

Our service scope includes real-time security event analysis, threat intelligence integration, use-case development, anomaly detection, and incident response processes. Additionally, we aim to make risks visible and provide actionable insights through regular vulnerability notifications, security recommendations, and detailed reporting. Organizational awareness and capabilities are further strengthened through trainings delivered by our expert cybersecurity engineers.

In addition to our SOC services, we offer SOAR (Security Orchestration, Automation, and Response) capabilities, enabling faster, more consistent, and automated incident response processes. By reducing manual workload in security operations, we significantly shorten response times and improve operational efficiency. As of 2025, our SOAR services achieved approximately 75% growth, reflecting strong customer demand for automation capabilities.

By the end of 2025, our SOC customer base had grown by approximately 40%, driven by both the expansion of existing services and the acquisition of new customers. Thanks to our shared SIEM and flexible service models, we have expanded our reach to organizations of varying scales, significantly increasing the effectiveness and inclusiveness of our SOC services. By keeping customer satisfaction at the core of our approach, we continue to sustain our growth and deliver high-quality services.

Turkcell Siber Portal:
The Siber Portal (Cyber Portal) was developed to provide SOC customers with a more efficient, transparent, and centralized service interface for monitoring and managing security operations. The platform enables the tracking of security alerts, visualization of operational metrics through interactive dashboards, and generation and sharing of security reports. In addition, it provides functionalities such as secure document sharing, asset and inventory management, a direct communication channel between SOC teams and customers, and the dissemination of security announcements and relevant information. Through the portal, users can review their security alerts in detail, follow analysis processes, and monitor incident response activities. This structure enhances visibility into security operations and enables faster, more effective management of security incidents.

Digital Forensics and Incident Response Service:
The Turkcell Digital Forensics and Incident Response (DFIR) Service has been fundamentally redesigned for 2025, integrating advanced Artificial Intelligence and Machine Learning to counter the velocity of modern cyber threats. Central to this evolution is the complete overhaul and strengthening of our SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) infrastructure. By transitioning to an AI-native SIEM, we now achieve hyper-granular visibility across hybrid environments, while our enhanced SOAR framework enables autonomous incident containment. These upgrades allow our expert engineers to sift through massive datasets in seconds, identifying "low-and-slow" attacks and lateral movements with unprecedented precision, effectively reducing response times from hours to milliseconds.

Drawing on a proven track record of investigating over 2,000 cyber incidents, our team now leverages these reinforced infrastructures to provide a more resilient defense for "open target" assets. The synergy between our upgraded automation engines and our engineers—who are now specialists in advanced Digital Forensics—ensures a comprehensive root-cause analysis for every breach. Beyond just identifying the "how" and "why" of an incident, our 2025 service model provides a predictive roadmap for recovery. We deliver deep-dive reports on the risks to customer data assets and business processes, implementing high-impact, AI-driven measures that ensure once a vulnerability is closed, it remains impenetrable against future recurrences.

Turkcell Purple Team Operations:
Throughout 2025, Turkcell significantly expanded its testing of attack techniques employed by advanced threat actors, fully aligning these efforts with the MITRE ATT&CK framework. In the second half of the year, the Purple Team conducted comprehensive simulations to assess the organization's cyber resilience, evaluate existing security controls, and proactively identify potential risk areas.

These activities concentrated on realistic attack scenarios targeting Active Directory, web applications, and critical systems. A combination of manual techniques and simulation platforms was utilized to prioritize threats with the potential to evade existing defenses or exhibit limited visibility. During these exercises, attack scenarios were re-executed, while concurrent analyses enhanced detection and response capabilities.

As a result, the security maturity of critical services was strengthened, defensive mechanisms were enhanced, and rapid responses were executed for high-risk vulnerabilities. Actionable insights derived from these exercises were applied to reinforce system security and elevate overall protection levels.

By continuously testing advanced attack scenarios and providing regular briefings to leadership, Turkcell has maintained a proactive security posture and consistently improved its resilience against the evolving threat landscape.

Cyber Threat Intelligence Team:
The purpose of this team is to monitor, analyze, and interpret emerging cyber threats, to support earlier warning and faster response, and to help the organization improve defensive decision-making before threats materialize into larger incidents. By combining intelligence production, monitoring, and closer alignment with operational response functions, the CTI team was designed to help reduce reaction time, improve situational awareness, and contribute to a more resilient digital environment.

Bozok Threat Intelligence Platform:
In 2025, the Bozok Threat Intelligence Platform underwent a significant structural transformation aimed at making the intelligence and detections produced by Turkcell more understandable, easier to access, and more actionable for its users. This transformation was important not only from a user-experience perspective, but also from an engineering perspective, because it created a more flexible foundation for further development. Bozok continued to evolve as a multi-capability threat intelligence environment covering key domains such as brand monitoring, VIP monitoring, attack surface management, vulnerability intelligence, and strategic intelligence. In practical terms, 2025 can be described as a foundational year in which the platform moved toward a more scalable and extensible structure that can better support both internal and external stakeholders. By the end of 2025, the platform was serving 84 customers, reflecting a growing operational footprint and reinforcing the need for a scalable, service-oriented intelligence delivery model.

Strategic Evolution of Ransomware Resilience: An Analytical Review of 2025 Defensive Frameworks and Operational Efficacy
The landscape of cybersecurity in 2025 continues to be defined by the pervasive and escalating threat of ransomware, which has transcended simple data encryption to become a multi-dimensional crisis affecting operational continuity, financial stability, and institutional reputation. The proliferation of the Ransomware-as-a-Service (RaaS) model has fundamentally altered the threat matrix by democratizing sophisticated attack capabilities, enabling even state-agnostic or low-technical actors to launch high-impact campaigns against critical infrastructures. In response to this evolving paradigm, the Cyber Defence Center (CDC) implemented a proactive and stratified defence strategy throughout 2025, moving beyond reactive incident response toward a model of systemic resilience. Central to this approach was the rigorous empirical validation of security controls, where a comprehensive analysis of 155 discrete ransomware variants revealed a 98.7% detection success rate. While 153 of these samples were preemptively neutralized by existing security architectures, the marginal 1.3% that bypassed initial filters triggered immediate remedial protocols, including the deployment of supplementary security controls and the closing of newly identified vulnerabilities. This iterative feedback loop between detection and remediation has been instrumental in hardening the organization's underlying security posture against zero-

day threats and sophisticated obfuscation techniques.
Furthermore, the integration of advanced Threat Hunting methodologies and Zero Trust Architecture (ZTA) has proven pivotal in identifying and mitigating latent risks before they escalate into full-scale breaches. By systematically analyzing SIEM (Security Information and Event Management) telemetry—specifically focusing on command-line artifacts, process hierarchies, and registry modifications—the CDC was able to verify the absence of unauthorized administrative tools or network reconnaissance activities within the corporate environment. This high level of visibility is complemented by a stringent overhaul of identity and access management policies, particularly targeting Remote Desktop Services (RDS) and compromised credential vectors, which remain the primary entry points for ransomware actors. These technical fortifications were harmonized with organizational readiness initiatives, including high-fidelity simulations and stress-testing of incident response reflexes, ensuring that the human element of the defence chain remains as robust as the technological one. As we transition into 2026, the findings from the 2025 fiscal year suggest that while the absolute elimination of ransomware risk is an impossibility, the systematic reduction of impact through high-velocity detection and architectural hardening has rendered these threats manageable. Moving forward, the focus will shift toward even more sophisticated predictive analytics to stay ahead of the next generation of autonomous and AI-driven ransomware threats.

Cyber Security Trainings:
Various trainings are provided by Turkcell cyber security engineers, who are experts in their fields, in order to increase the information security awareness of corporate customers at Turkcell CDC. In 2025, our team placed a strong emphasis on the individual development of employees, in addition to the training programs provided. In this context, team members completed globally recognized cybersecurity courses through various online learning platforms. Special focus was given to enhancing the detection and threat hunting capabilities of DFIR (Digital Forensics and Incident Response) personnel, and all training activities were planned to align with real-world incident response requirements.

Throughout the year, a series of cyber incident response exercises simulating realistic attack scenarios were conducted. These exercises required participants to perform all phases of incident management—including detection, prioritization, threat hunting, containment, and reporting—within defined timeframes. These activities significantly contributed to strengthening our cyber resilience and advancing DFIR capabilities, forming a key part of our 2025 cybersecurity workforce development strategy.

Looking ahead to 2026, our organization plans to expand its focus toward AI-driven and cloud-focused cybersecurity capabilities. This includes increasing expertise in cloud security monitoring, cloud-native threat detection, and incident response in cloud environments, as well as leveraging AI to enhance detection engineering, automated threat hunting, and intelligent incident response, further improving operational efficiency and threat detection accuracy.

Achievements

Locked Shields, the world's largest live-fire cyber defense exercise organized by the NATO Cyber Defence Cooperation Centre of Excellence (CCDCOE), brought together approximately 4,000 cybersecurity experts from 41 countries. We are proud to announce that our Blue Team represented our country in the Digital Forensics category. With the contributions of our experts, our country achieved 2nd place among the 21 competing teams. We are truly proud!

ABOUT ORGANIZATION

Turkcell is a converged telecommunication and technology services provider, founded and headquartered in Turkey. Turkcell CDC is the Cyber Defence Center of Turkcell. Turkcell CDC provides variety of services in the Information Security domain at national and international scale including threat intelligence, managed security operations center and DFIR services. Moreover, Turkcell CDC provides the Digital Security Service for individual Turkcell customers. With this service the customers are protected from various types of phishing and fraud attacks as well as credential leakage.

Turkcell CDC is part of the Turkcell Cyber Security Directorate. Within the Cyber Security Directorate, apart from the above services, DDOS tests and managed DDOS Protection Services, sales, installation and integration of network security products, Identity Access Management Service, Continunious Vulnerability Services, Attack Surface Management Services, MDR/XDR Services, SIEM Consultancy are also provided.

2026 PLANNED ACTIVITIES

Bozok Threat Intelligence Platform:
For 2026, the primary objective for Bozok is to improve the quality, consistency, and operational usefulness of existing modules rather than expanding scope without discipline. The platform vision is to deliver outputs that help users take proactive action, not merely consume raw data. This means improving login and access experience, increasing the clarity and reliability of notifications and alerts, strengthening dashboard and export capabilities, and presenting intelligence in a more decision-oriented format. At the same time, module-level improvements are planned across brand monitoring, VIP monitoring, attack surface management, vulnerability intelligence, and strategic intelligence so that each area produces more relevant, timely, and actionable results for customers and internal security teams. In parallel, a controlled AI-assisted experience is planned to increase accessibility of intelligence content while maintaining safety, traceability, and practical value.

Cyber Threat Intelligence Team:
In 2026, the CTI team aims to mature from an emerging function into a more structured intelligence production capability with repeatable processes, stronger data governance, and closer integration with operational defence teams. The focus areas include standardizing intelligence production, publishing regular threat actor and TTP-focused analyses, improving IOC lifecycle management, and building a stronger data backbone through STIX-based modeling and enrichment. Another

important goal is to strengthen the DFIR feedback loop so that intelligence is not only produced, but also consumed through concrete actions such as hunting, detection improvement, incident support, and defensive prioritization. In addition, the team plans to use automation and LLM-assisted workflows in a controlled manner to reduce manual effort, accelerate enrichment, and support persona-based intelligence outputs such as regular bulletins, strategic reporting, and decision-ready summaries for technical and executive audiences.

2026 Strategic Direction in One View

Across both Bozok and the CTI team, the 2026 direction can be summarized in four themes: operational intelligence production, a stronger and more centralized data backbone, higher-value platform outputs, and selective AI enablement. The target is not simply to add new features, but to deliver intelligence that is easier to trust, easier to consume, and easier to convert into action. This reflects a broader vision of strengthening cyber resilience through better prioritization, more usable intelligence products, and closer alignment between intelligence, detection, response, and customer-facing value creation.

Turkcell & Google Cloud Partnership

As cyber threats continue to grow in complexity and scale, Turkcell positions the development of world-class security operations capabilities as a strategic priority. In this direction, we aim to deliver innovative and scalable cybersecurity solutions by strengthening our focus on Google Cloud technologies.

As Turkey's leading national contractor and an authorized Google partner, our 2026 vision focuses on the effective operationalization of the Google SecOps platform, advancing our threat intelligence capabilities, and increasing internationally certified in-house expertise as key priorities.

Aligned with this vision, we aim to maintain our position as a trusted solution partner at both national and international levels by adopting a proactive, integrated, and sustainable cybersecurity approach.

In this context, Security Operations (SecOps) serves as the central pillar of our 2026 cybersecurity strategy. By leveraging Google's Chronicle Security Operations platform—an industry-leading SIEM/SOAR solution built on petabyte-scale data infrastructure—we aim to significantly enhance our threat detection, investigation, and response capabilities.

AI-Driven Cybersecurity Initiatives and Future Vision:

During the past year, various initiatives have been implemented to enable more effective use of artificial intelligence in cybersecurity operations. In this context, AI-supported cyber agenda monitoring solutions were developed to ensure that critical cybersecurity developments can be followed more quickly, clearly, and in a prioritized manner; structures aimed at accelerating the analysis of phishing emails were studied; and capabilities were established to produce more comprehensive technical outputs in malware static analysis and reverse engineering processes through multi-agent architectures. In addition, approaches were developed to monitor current threat landscape developments through social media and open-source data, transforming them into meaningful cyber events and thereby enhancing the operational awareness of analyst teams. In the coming period, these AI-supported cybersecurity capabilities are planned to be further

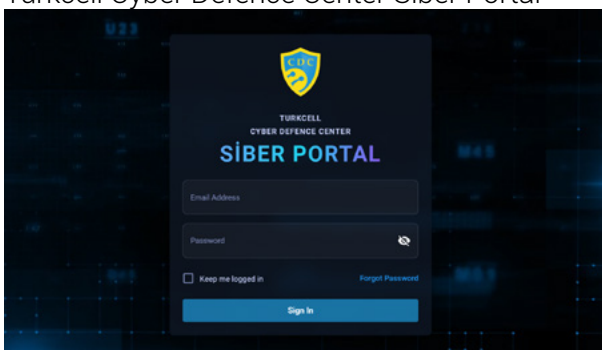
matured. In this regard, the focus will be on behavioral anomaly detection and threat hunting studies aimed at identifying suspicious activities on critical systems in a more proactive manner, as well as on next-generation analyst assistant approaches capable of producing end-to-end analysis on an incident basis. The objective is to establish an AI-based capability domain that reduces analyst workload, increases assessment speed, leverages institutional knowledge more effectively, and contributes to faster, more consistent, and sustainable action against cyber threats.

CONCLUSION

In 2025, Turkcell demonstrated its leadership in technology and innovation on the ground. We reinforced our pioneering role in 5G while elevating both our technological infrastructure and operational capabilities through strategic partnerships with Google Cloud. Across the organization and within the Turkcell CDC, we integrated artificial intelligence into our processes, achieving significant gains in efficiency, speed, and analytical decision-making.

Innovation is not just a goal—it is embedded in our DNA. Both our vision and mission are driven by a strong motivation to embrace change and adopt cutting-edge technologies. Building on the momentum we achieved in 2025, we aim to propel it even further in 2026, strengthening our leadership position in the industry through a proactive, innovation-focused, and strategically driven approach.

Turkcell Cyber Defence Center Siber Portal



BOZOK Cyber Threat Intelligence Platform

Turkcell Cyber Defence Center – Videowall

HUAWEI (HWT)

HIGHLIGHTS OF 2025

Summary of Major Activities

Continuously Strengthening Cyber Security, AI Governance, and Data Protection

In 2025, Huawei continued to enhance our end-to-end cyber security assurance system and AI governance framework, contributing to the broader cyber security ecosystem through collaboration with industry partners, standards bodies, and regional stakeholders. We have formulated our AI business intent, governance principles, and an AI governance framework that aligned with international standards, embedding principles of transparency, traceability, security, robustness, and accountability across engineering and operational processes.

We strengthened data security governance through comprehensive data classification, protection mechanisms, and lifecycle-based compliance controls. Dedicated personal data protection systems were further enhanced to ensure secure and lawful processing of data across global operations. In parallel, we advanced open-source software security governance to improve vulnerability management, software integrity, and secure lifecycle management.

Enhancing Operational Security and Supply Chain Resilience

We reinforced operational resilience across global service delivery through improved network change management, security monitoring, and risk control mechanisms. In 2025, our systems supported more than 1.25 million network change operations globally, improving operational stability and reducing cyber risk exposure.

We also strengthened supply chain security through structured supplier cyber security assessments, admission testing, and capability development programs. These initiatives enhanced resilience across the broader ICT ecosystem, including partners and suppliers operating within OIC member environments.

Supporting Industry Collaboration and Capacity Development

Huawei continued active collaboration with international standards organizations, CERT communities, telecommunications operators, and government stakeholders. We supported cyber security awareness programs, training initiatives, and joint resilience exercises, contributing to improved cyber security readiness across multiple regions.

As the commercial member of OIC-CERT, Huawei continuously contribute to the institution with its technical knowledge and expertise. In early 2025, Huawei as the co-chair of OIC-CERT Supply Chain Working Group has co-developed and released the OIC-CERT Software Supply Chain Framework. Huawei also stands by the OIC- COMSTECH in strengthening cybersecurity for OIC member states. Huawei has supported COMSTECH in holding the annual cyber security workshop and delivered presentation on AI security and critical information infrastructure security.

OIC-COMSTECH International Workshop on AI and Cybersecurity

Achievements

- In 2025, we achieved more than 890 security and privacy certifications globally, including over 300 new certifications during the year. These covered international standards such as ISO, Common Criteria, EU regulatory frameworks, and national cryptography requirements, reflecting our continued commitment to compliance and assurance.
- We actively contributed to global standardization efforts, submitting more than 880 proposals to organizations such as 3GPP and GSMA. We also contributed to ISO/IEC, ETSI, IETF, and TC260 in areas including AI security, confidential computing, and post-quantum cryptography, supporting secure digital transformation across ecosystems including OIC-CERT member countries.
- Our cloud services maintained secure and stable operations for more than 900 consecutive days while defending against hundreds of billions of cyber-attacks. AI-driven security systems achieved a 95% detection rate for unknown threats.
- We strengthened supply chain security by conducting assessments for more than 4,000 suppliers and performing security testing on materials from over 180 suppliers. More than 2,000 supplier personnel completed cyber security training.
- Our contributions were recognized through multiple international awards, including cybersecurity excellence and industry development honors in Thailand, Nigeria, and the Arab region. In Indonesia, Huawei remains committed to strengthening the country's cyber security ecosystem through collaboration, innovation, and industry engagement, which earned it the Public-Private Partnership Award at the National Cybersecurity Connect 2025. In the UAE, Huawei is presented the Most Valuable Partner Award in recognition of its long-term commitment and contributions to the development of local cyber security talent, professional capabilities, and ecosystems.
- For detail of Huawei's cybersecurity achievements in 2025, please refer to the Huawei 2025 ANNUAL REPORT (Page 81-87): https://www.huawei.com/en/annual-report/2025

ABOUT ORGANIZATION

Huawei is a leading global provider of information and communications technology (ICT) infrastructure and smart devices. The company has more than 208,000 employees, and operates in more than 170 countries and regions, serving more than three billion people around the world. In the past 30-plus years, Huawei has worked with carriers to build over 1,500 networks and helped millions of enterprises go digital. In addition, Huawei has shipped tens of millions of sets of intelligent automotive components, and HarmonyOS is now running on over one billion devices. Whether for connectivity or devices, Huawei has always maintained a solid track record in security. Huawei has operated in the Middle East region for over 20 years, with Bahrain as the regional headquarters and the UAE as the MEA business centre.

Over the past year, cutting-edge technologies such as AI, 5.5G, and quantum computing have accelerated digital and intelligent transformation across industries. While these advancements boost economic growth, the rapid expansion of digital assets has increased network exposure, heightening cyber security and privacy risks. Emerging technologies introduce new threat vectors, and the complexity of hardware and software supply chains continues to grow. As a result, ensuring cyber security and privacy protection remains an ongoing challenge.

Huawei believes that cyber security and privacy protection are the cornerstones of the digital and intelligent world. Huawei strives to tackle the challenges and seize the opportunities that accompany technological transformations through managerial improvement, technological innovation, and open collaboration. Huawei works hard to hone our competitive edge in security, take concrete steps to manage related risks, and work alongside our customers, suppliers, and partners to strengthen cyber security and privacy protection capabilities. Through these actions, Huawei is committed to creating a better life for all in the future digital and intelligent world.

Huawei has identified and prioritized cybersecurity since 2005 when the Huawei Product Security Incident Response Team (PSIRT) is formed. PSIRT manages the receipt, investigation, internal coordination, and disclosure of security vulnerability information related to Huawei offerings and it is an important window to disclose the vulnerability of Huawei products. Huawei PSIRT became a FIRST member in 2010 and adheres to ISO/IEC 29147:2018 and ISO/IEC 30111:2019.

ACTIVITIES & OPERATION

Scope and definitions

In 2025, Huawei continued strengthening its cyber security operations through continuous improvement in governance, operational processes, technological innovation, and industry collaboration. These efforts have allowed us to strengthen our competitive edge in product and solution security, and we are continuing to work closely with our customers, partners, and suppliers to develop the cyber security and privacy protection capabilities needed to safeguard the digital and intelligent world.

Incident handling and response operations

Huawei continued integrating security-by-design principles into operational processes, including AI governance, vulnerability management, software integrity protection, and data lifecycle security management.

Huawei continued enhancing its cyber threat detection and incident response capabilities across cloud and network environments. In 2025, Huawei Cloud maintained secure and stable operations for more than 900 consecutive days without major security incidents while defending against hundreds of billions of cyber-attacks targeting infrastructure and digital services.

AI-driven threat detection and security analytics capabilities were further enhanced to improve identification of ransomware activities, phishing campaigns, malicious applications, and advanced persistent threats. Operational improvements increased the detection rate for unknown threats to 95%, enabling faster mitigation of emerging attack patterns.

Publication(s)

Huawei contributed to industry knowledge sharing through cyber security publications, technical frameworks, and operational best practice documentation. These contributions supported improved understanding of cyber resilience, AI security governance, data protection, and secure operational management. In 2025, we released the Huawei Data Security Governance Practices to provide structured frameworks and practical guidance for strengthening enterprise-level data protection. We also co-published the Qiankun Intelligent Automotive Solution Cyber Security White Paper, outlining security governance and resilience strategies for intelligent connected vehicle ecosystems.

New service(s)

In 2025, Huawei continued enhancing its security capabilities and service offerings to address evolving cyber threats targeting AI platforms, cloud environments, intelligent networks, and digital infrastructure ecosystems including:

- Huawei introduced enhanced AI-driven security capabilities to strengthen protection across cloud platforms, intelligent networks, AI applications, and digital ecosystems. New security technologies included deepfake face detection capabilities designed to identify, warn against, and block fraudulent applications and AI-enabled scams.
- New quantum-safe transmission capabilities incorporating OTN encryption, Xsec encryption, and post-quantum cryptography technologies were introduced to strengthen protection against emerging quantum computing threats.
- Huawei Cloud launched the Large Model Security Solution to strengthen security and compliance throughout the lifecycle of AI model training, deployment, and operational use. The solution enabled intelligent collaborative defense capabilities and supported secure operations for large-scale AI environments facing sophisticated cyber threats.

- Huawei also introduced the Security Agent platform to improve unified security operations across hybrid, multi-cloud, and on-premises environments. AI-driven analytics and automated response capabilities significantly improved threat analysis and operational response efficiency, enabling centralized and visualized security management across distributed ICT environments.

EVENTS ORGANIZED & INVOLVEMENT

In 2025, Huawei collaborated with industry partners and stakeholders to conduct cybersecurity events globally, promoting cyber security awareness, resilience, and best practices.

- **UAE:** Co-hosted the "Imagine Wi-Fi 7 to Reality" launch event with IEEE UAE Section in conjunction of GITEX GLOBAL 2025, and jointly released the campus security network construction standards for the education industry.; Together with TDRA and DGOV, held a cyber security workshop on cyber security trends, supply chain security, post-quantum security, and AI security.
- **Pakistan:** Held the Next-Gen Cyber Resilience Workshop & Telecom Cyber Security Summit with the Pakistan Telecommunication Authority (PTA)
- **Saudi:** Participated in the cyber security workshop held by the National Cyber Security Authority (NCA); Assisted in building the Hemaya cybersecurity ecosystem, conduct cybersecurity training and communication activities.

2026 PLANNED ACTIVITIES

In 2026, Huawei will continue strengthening cyber security governance, AI security, and privacy protection capabilities while deepening collaboration with global partners, including CERT communities and regional organizations such as OIC-CERT.

We will further enhance AI-driven threat detection, ransomware defense, cloud security operations, and post-quantum cryptography readiness. Continued investment will be made in secure digital infrastructure, intelligent security operations, and supply chain resilience.

Huawei will also expand collaboration in cyber security training, standards development, and joint innovation initiatives to support the development of secure, resilient, and trusted digital ecosystems globally. Given the rapid development of AI technology, OIC-CERT members need to gain deep-dive insights into AI risks and consider to develop the AI governance framework. Huawei and other OIC-CERT members will work closely to address AI security concerns and to raise awareness, in the meanwhile sharing experience of AI governance framework and capabilities.

CONCLUSION

In 2025, Huawei strengthened its cyber security capabilities and contributed to global cyber resilience through collaboration with industry stakeholders, standards organizations, and CERT communities, including OIC-CERT-related cooperation.

We remain committed to supporting secure digital transformation through continuous improvement in cyber defense capabilities, standards contribution, and collaborative security initiatives. Through ongoing cooperation and knowledge sharing, we aim to contribute to a more secure and resilient global cyber security ecosystem.

PROFESSIONAL MEMBERS

DR. ABDULRAHMAN ABDU MUTHANA / SMART SECURITY SOLUTIONS

HIGHLIGHTS OF 2025

Summary of Major Activities

- Presenting Cybersecurity seminars on developing cybersecurity programs curriculums in higher education utilizing NICE standard framework
- Implementing Cybersecurity compliance program for ITSM Company
- Development of cybersecurity training platform CTF (Capture The Flag) for cybersecurity students
- Research on integrating AI in Malware detection and prevention
- Implementing a national cybersecurity awareness program
- Digital Forensics of Malicious Email Incidents in local bank

Achievements

- Providing certification preparation training for a number of Cybersecurity professionals in CEH, ECIH, & CPENT courses
- Planning and implementing of information security programs for a number of governmental organizations
- Developing a Secure local social platforms for Educational institutions
- Presenting a series of seminars on developing Job-Ready Cybersecurity Capabilities utilizing NICE standard framework
- Presenting a series of seminars on developing cybersecurity curriculums in higher education utilizing NICE standard framework
- Implementing role-based Cybersecurity awareness programs for CEOs, and employees in different IT companies

ABOUT ORGANIZATION

Smart Security Solutions Company (SMARTSEC) is the first company in Yemen for providing Information Security training, consultancy, and Information Security research. Dr.Abdulraman Muthana and a group of Information security professionals founded SMARTSEC on October 2010

ACTIVITIES & OPERATION

Scope and definitions

Cybersecurity Governance, Cybersecurity Defence, training, penetration testing, malware detection and prevention, Cybersecurity solutions

Publication(s)

- "Human Factors in Social Engineering attacks", prepared.
- "An efficient solution for detecting and defending ransomware", sent

New service(s)

- Social networks Privacy Advisor
- Secure local social platforms for educational institutions

EVENTS ORGANIZED & INVOLVEMENT

Events organized by the organization / agency

- Implementing role-based Cybersecurity Awareness Training for All personnel, IT-staff, and CEOs in different IT companies
- Presenting Cyber Security Seminars on NICE Cybersecurity framework and tools
- Implementing Cyber Security Training for certification preparation

Events involvement

- Participating in a national workshop on building national cybersecurity capabilities that was sponsored by national academic accreditation council in cooperation with Al-Razi University, and held on July 29th 2025, Sanaa, YEMEN.
- Participating in Technology and Innovation Exhibition (SMART-EX-2025), sponsored by the Ministry of Communications and the Yemeni Telecommunications Union ITU, and held between August 10th and August 14th 2025, Sanaa, YEMEN

2026 PLANNED ACTIVITIES

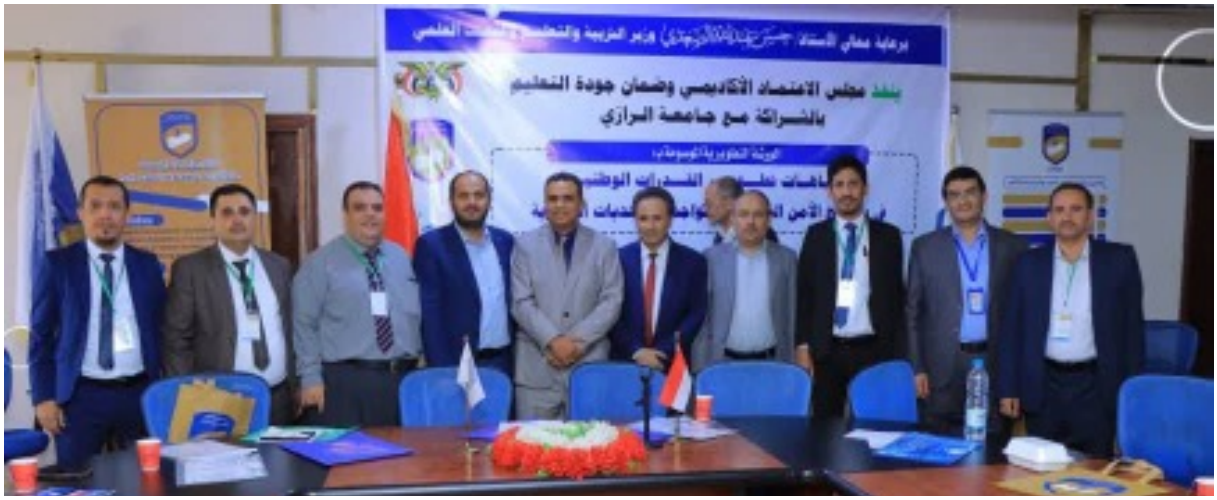
- Continuation of implementing a country-wide cybersecurity awareness program in cooperation with telecommunication network operators
- Continuation searching in integrating Artificial Intelligence and cybersecurity for development of Anti Malware solutions
- Expansion of SMARTSEC to include a dedicated department for Cybersecurity compliance consultancies and services.
- Training Plan for SMARTSEC staff.
- In-house Development of special purpose Malware Investigation Tools.

CONCLUSION

The team at SMARTSEC is dedicated to raising the level of cybersecurity in Yemen by spreading cybersecurity awareness and training cybersecurity professionals in different cybersecurity specializations required by the country and region. Additionally, the company provides cybersecurity consulting services to academic institutions to improve the quality of cybersecurity education as well as public and private sectors to protect Yemen's technological infrastructure. All activities and operations of the team members toward a single goal: advancing up the level of cybersecurity in Yemen to serve our country and society.

A seminar on developing cybersecurity curriculums in higher education insititutions utilizing NICE standard framework presented by the CEO of SMARTEC, Dr. Abdulrahman Muthana, at national academic accreditation council, Sanaa, Yemen (29-07-2025).

Dr. Abdulrahman Muthana, CEO of SMARTEC, with the President of Al-Razi University, Prof. Khalil Al-Wajeeh and some members of the workshop organizing team, at national academic accreditation council, Sanaa, Yemen (29-07-2025).



A siminar on developing Job-Ready Cybersecurity Capabilities using NICE framework targeting private and public sector companies by Smart Security Solutions (SMARTEC) at SMART-EX-2025, Sanaa,Yemen (10-08-2025)

A siminar on developing Job-Ready Cybersecurity Capabilities using NICE framework categories and workroles presented by the CEO of SMARTEC, Dr. Abdulrahman Muthana, at SMART-EX-2025, Sanaa,Yemen (10-08-2025)

OIC-CERT Permanent Secretariat:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

secretariat@oic-cert.org
www.oic-cert.org