OIC-CERT
Computer Emergency Response Team

OIC-CERT 2022 ANNUAL REPORT

Organization of the Islamic Cooperation
Computer Emergency Response Team

This page is purposely left blank

The OIC-CERT Annual Report 2022

Azerbaijan

Bangladesh

Brunei Darussalam

Indonesia

Jordan

Kyrgyzstan

Libya

Malaysia

Nigeria

Oman

Pakistan

Somalia

Tunisia

Turkeye

United Arab Emirates

Uzbekistan

Yemen

Singapore

ACRONYMS

A

AITI	Authority for Info-communications Technology Industry (*Brunei*)
APCERT	Asia Pacific Computer Emergency Response Team

B

BSSN	Badan Siber dan Sandi Negara / National Cyber and Crypto Agency (*Indonesia*)

C

CBJ	Central Bank of Jordan
CII	Critical Information Infrastructures
CRI	International Counter Ransomware Initiative
CTF	Capture the Flag
CTI	Computer telephony integration
CSC	Cybersecurity Council (UAE)
CSIRT	Computer Security Incident Response Team
CSIS	Cybersecurity Innovation Series
CSB	Cyber Security Brunei
CSF	Cybersecurity Strategy for the Financial and Banking Sector (Jordan)
CSM-ACE	Cyber Security Malaysia – Award, Conference & Exhibition

E

EGNC	E-Government National Centre (*Brunei*)

F

FIA	Federal Investigation Agency
FinCERT	Financial Computer Emergency Response Team
FIRST	Forum of Incident Response and Security Teams

G

GCC	Gulf Cooperation Council
GISEC	Gulf Information Expo & Conference

I

ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
Id-SIRTII/ CC	Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center
IOCs	Indicator of Compromises
ISAC	Information Sharing and Analysis Centre
ISO/ IEC	International Organization for Standardization/ the International Electrotechnical Commission
ISP	Internet Service Provider
ITSA	IT Security Assessment
ITU-ARCC	ITU-Arab Regional Cybersecurity Centre

L

LEA	Law enforcement agency
LSN	Lembaga Sandi Negara / National Crypto Agency (*Indonesia*)

M

MDR	Medical Device Reporting
MISP	Malware Information Sharing Platform
MoU	Memorandum of Understanding
MTCP	Malaysian Technical Cooperation Program

N

N-CERT	National CERT (*Bangladesh*)
NCCA	National Cyber & Crypto Agency (*Indonesia*)
NDA	Non-Disclosure Agreement
NEPRA	National Electric Power Regulatory Authority (*Pakistan*)
NISSA	National Information Security & Safety Authority (*Libya*)

P

PSIRT	Product Security Incident Response Team

R

RBPF	Royal Brunei Police Force

S

SWIFT	Society for Worldwide Interbank Financial Telecommunication

U

UTeM	Technical University Melaka

W

WG	Working Group
WZPDCL	West Zone Power Distribution Company (*Bangladesh*)

THE CHAIRMAN’S STATEMENT

“… collaboration and working together will lead to achieving results that are more significant.”

Dear Members of the OIC-CERT,

It is my pleasure to welcome you all to the OIC-CERT Annual Report 2022. As the Chairman of this organization, I am honoured and delighted to present the OIC-CERT’s achievements and progress collectively made along with the OIC-CERT members

In alignment with the vision of the OIC-CERT to be a leading international cybersecurity platform to make the world having a safer cyber space and the mission to develop cybersecurity capabilities to mitigate cyber threats by leveraging global collaboration, I am proud to say that we have made significant strides in achieving this goal. The OIC-CERT Board Members as well as individual member countries and partner's dedication and commitment have resulted in remarkable achievements

This annual report highlights our collective achievements in 2022, including the successful implementation of innovative cybersecurity solutions and projects, the establishment of strategic partnerships and alliances

As we continue to face new and complex challenges, it is imperative that we work together to develop innovative solutions that can address these challenges effectively. The organization believes that by collaboration and working together will lead to achieving results that are more significant

In conclusion, I would like to thank everyone who has contributed to the success of the OIC-CERT as well as to the development of this report, including the members, partners, OIC-CERT Secretariat and Board Members

Eng. Badar Ali Al-Salehi
Director, Oman National CERT
Information Technology Authority
Sultanate of Oman.

ABOUT THE OIC-CERT

The Organization of the Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**) 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 their national CERTs

Membership

As of Jan 2023, the OIC-CERT has a network and strategic collaboration with **61** members from **28** OIC countries**.** This alliance is further supported through the presence of **7** Commercial Members, **5** Professional Members, **3** Fellow Member, **1** Affiliate Member, and **1** Honorary Member

The Full Membership

These are CERTs, Computer Security Incident Response Teams (**CSIRT**s) 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 Centre (**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 Crypto 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 Qatar - Qatar Computer Emergency Response Team (**Q-CERT**)
20 Saudi Arabia - Saudi Arabia Computer Emergency Response Team (**CERT-SA**)
21 Somalia - Somalia Computer Emergency Response Team (**SomCERT**)
22 Sudan - Sudan Computer Emergency Response Team (**SudanCERT**)

23 Syria - National Agency for Network Services

24 Tunisia - National Agency for Computer Security (**tunCERT**)

25 Türkiye - National Cyber Security Incident Response Team (**TR-CERT**)

26 United Arab Emirates - UAE Computer Emergency Response Team (**aeCERT**)

27 Uzbekistan - Uzbekistan Computer Emergency Response Team (**UzCERT**)

The General Membership

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

1 Bangladesh
- BangladeshCERT
- Bangladesh Computer Emergency Response Team (**bdCERT**)

2 Iran
- Isfahan University of Technology Computer Emergency Response Team (**IUTcert**)
- Amirkabir University of Technology Computer Emergency Response Team (**AUTcert**)
- Sharif University of Technology Computer Emergency Response Team (**SharifCert**)
- Shiraz University ICT Center (**SUcert**)
- Maher Center
- APA Ferdowsi University of Mashhad CERT (**APA-FUMcert**)
- APA University Bojnord CERT (**APA-UBCERT**)

3 Jordan
- Unit of Financial Computer Emergency Response Team (**JoFin-CERT**)

4 Kazakhstan
- Center for Analysis and Investigation of Cyber-Attacks (**CAICA**)

5 Kyrgyzstan
- Computer Emergency Response Team **(cert.ict kg)**

6 Malaysia
- Universiti Teknikal Malaysia Melaka (**UTeM**)

7 Pakistan
- Pakistan Information Security Association (**PISA-CERT**)

8 Türkiye
- Türkiye Cyber Security Incident Response Team (**TR-CSIRT**)

9 Uganda
- Uganda Computer Emergency Response Team (**UG-CERT**)

10 Uzbekistan
- Inha University in Tashkent

The Affiliate Membership

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

The United States

- Team Cymru

The Commercial Membership

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

1 Malaysia
- Serba Dinamik Group Berhad
- FNS (M) Sdn. Bhd

2 Oman
- Insight SOC

3 South Korea
- Duzon

4 Singapore
- CERT-GIB

5 Türkiye
- Turkcell CDC

6 United Arab Emirates
- Huawei (**HWT**)

The Professional Membership

These are individual experts in information security area that would like to contribute to the collaborative platform. Professional Members' sole purpose is to give expert advice pertaining to the OIC-CERT and information security related matter

1 Malaysia
- Mr. Hatim Mohammad Tahir
- Prof. Dr. Rabiah Ahmad- *Universiti Teknikal Malaysia Melaka*
- Abdul Fattah Mohamed Yatim- *Teknimuda (M) Sdn Bhd*
- Dr. Sofia Najwa Ramli– *Universiti Tun Hussein Onn Malaysia*

2 Yemen
- Dr. Abdulrahman Ahmad Abdul Muthana - *Smart Security Solutions*

The Fellow Membership

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

1 Tunisia
- Prof. Nabil Sahli

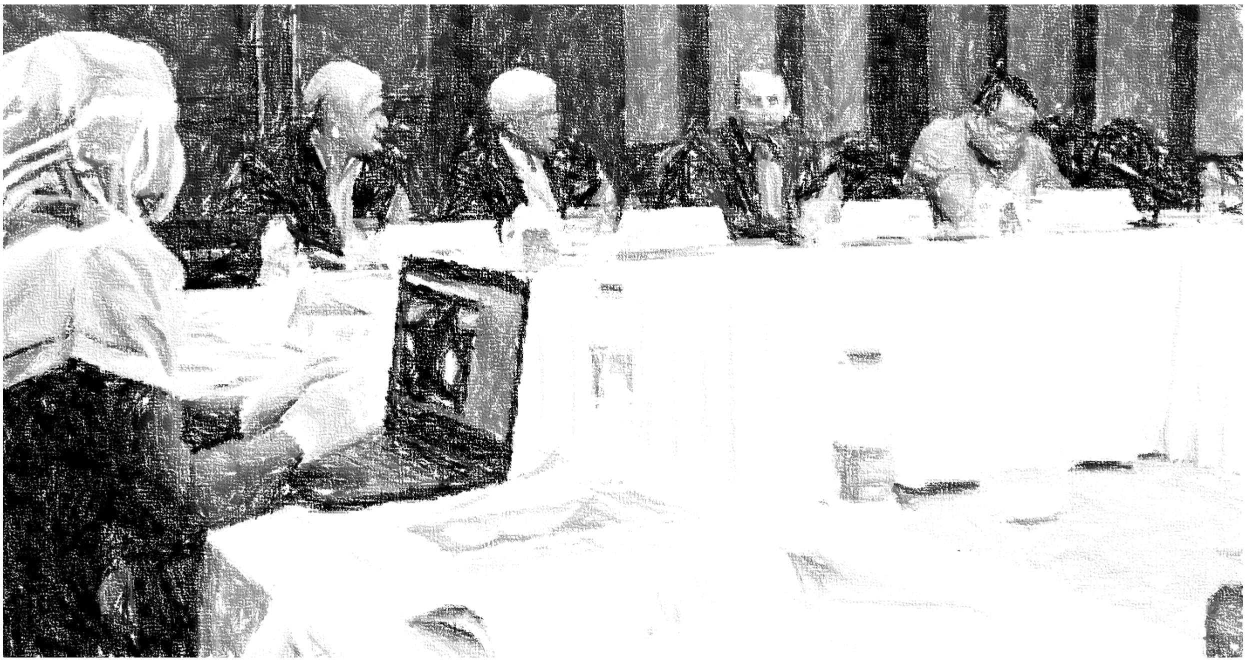
2 Malaysia
- Assoc. Prof. Colonel (R) Dato' Ts. Dr. Husin Bin Jazri
- Ts. Dr. Zahri Yunos

The Honorary Membership

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

Saudi Arabia

- Organization of the Islamic Cooperation



SECRETARIAT UPDATES

OIC-CERT MEMBERSHIP – NEW MEMBERS

As of Jan 2023, OIC-CERT has 61 members from 28 OIC members countries which consist of 27 Full Members, 17 General Members, 7 Commercial Members, 5 Professional Members, 3 Fellow Members, 1 Affiliate Member, and 1 Honorary Member

In 2022, five (5) new organizations/ agencies/ individuals became OIC-CERT member

Full member	National Cyber Security Center (NCSC), Bahrain
General member	Uganda Computer Emergency Response Team (**UG-CERT**), Uganda Inha University in Tashkent, Uzbekistan Unit of Financial Computer Emergency Response Team (**JoFin-CERT**), Jordan
Fellow member	Ts. Dr. Zahri Yunos, Malaysia

Membership Management Portal

The portal was developed by the Azerbaijan Government CERT (**AZ.GOV.CERT**). The objective of the portal is to manage information of each OIC-CERT member. In the future, all the membership processes will be done through this portal

OIC-CERT Activities

Meetings

OIC-CERT Board Meeting

Five (5) OIC-CERT Board meetings were conducted in 2022

• Board No. 1/2022	10 Feb 2022 (online)
• Board No. 2/2022	27 Apr 2022 (online)
• Board No. 3/2022	26 Jul 2022 (online)
• Board No. 4/2022	17 Oct 2022 (online)
• Board No. 5/2022	6 Nov 2022 (Physical | Muscat, Oman)

OIC-CERT 10th General Meeting & 14th Annual Conference

The OIC-CERT 10th General Meeting & 14th Annual Conference (in conjunction with the 10th Regional Cybersecurity Summit & the Forum of Incident Response and

Security Teams (**FIRST**) & ITU-ARCC Regional Symposium for Africa and Arab Regions) was organized on 6 – 9 Nov 2022 in the Sultanate of Oman

The theme for 2022 Annual Conference is *Cybersecurity Innovation and Industry Development*

At the OIC-CERT 10th General Meeting, the new Board Members were elected. The Board Members for the term 2022-2024 are

- OCERT (Oman) - Chair
- NCCA (Indonesia) - Deputy Chair
- aeCERT (UAE) – Deputy Chair
- CyberSecurity Malaysia (Malaysia) - Permanent Secretariat
- CERT.GOV.AZ (Azerbaijan)
- BRUCERT (Brunei)
- EG-CERT (Egypt)

The OIC-CERT Cyber Drill

The OIC-CERT Cyber Drill 2022 was successfully conducted to test the response capabilities of the participating teams. It was held on 7 Nov 2022 with theme entitled *The Rapid Evolving of Cyber Threats Landscape in Parallel with Innovation in Cybersecurity Industry* hosted by OCERT, Oman.

Capacity Building

Online Training

Twelve (12) trainings were organized in 2022 by Egypt, Indonesia, Malaysia, Brunei, Group-IB, Huawei and UTeM

- 5G Security Framework Workshop (Huawei & Malaysia) - 22 Feb
- Information Sharing and Analysis Centre Webinar (Malaysia) - 17 Feb
- *Arms Race: The Use of Neural Network Technology by Fraudsters* Webinar (Group-IB) - 29 Mar
- *Certified Penetration Tester* Training under the Malaysian Technical Cooperation Programme (**MTCP**) (Malaysia) - 17-20 & 23-26 May
- *Analysing Network Artifacts* Workshop (Egypt) - 16-17 May
- *Certified Penetration Tester* Training under the MTCP (Malaysia) - 14-17 & 20-21 Jun
- *Managing Security Operation Centre (**SOC**) in Government Sector* Webinar (Indonesia) - 19 Jul
- *Network Forensics* Technical Workshop (Indonesia) - 12-13 Jul
- *Risk & Threat Analysis on Internet of Everything* (IoE) (Malaysia) - 1 Aug

- *Analysing Operating System Artifacts* Workshop (Egypt) - 29-30 Aug
- *Digital Security Professional Development & Lifelong Learning Program* under the MTCP (Malaysia) - 23-26 & 29-30 Aug
- *Global Digital Security and Forensic 2022 - Future & Trends Government Sector: Emerging Threats in Social Media: Technology and Policy* Webinar (UTeM) - 26 Oct

The Malaysian Technical Cooperation Programme

In 2022, Malaysia organized 3 online trainings under the MTCP involving 33 participants from 20 MTCP recipient countries

- Certified Penetration Tester (CPT)

  Session 1: 17-20 & 23-24 May 2022
  Involving 12 participants from Bangladesh, Philippines, Sri Lanka, Turkmenistan, Uzbekistan & Vietnam

  Session 2: 14-17 & 20-21 Jun 2022
  Involving 10 participants from Algeria, Argentina, Azerbaijan, Comoros, Ecuador, Jordan, Morocco, Sudan, Tanzania & Zimbabwe
- Digital Security Professional Development & Lifelong Learning Program (ADS): 23-26 & 29-30 Aug 2022
  Involving 11 participants from Cambodia, Malawi, Mauritius, Morocco, Nepal & Sudan

Publication and Procedures

OIC-CERT Journal of Cyber Security

The 4th volume has been published in 2022 consisting of 7 papers from Azerbaijan, Indonesia, Malaysia, Huawei, and UAE

The OIC-CERT Journal of Cyber Security (OIC-CERT JCS) is now accepting submissions for Volume 5

Kindly refer to *https://www.oic-cert.org/en/call-for-paper.html*. The Secretariat invites submission of manuscripts for the next edition of the journal from cybersecurity professionals, scholars, and practitioners

The OIC-CERT JCS is a peer-reviewed journal that aims to produce quality papers in the vast field of cybersecurity utilising a ready pool of cybersecurity professionals either from the industry or the academia among the OIC-CERT and the OIC member countries. Currently, this journal is indexed in Google Scholars

OIC-CERT Annual Report 2021

The Secretariat in May 2022 has published the OIC-CERT Annual Report 2021. The Annual Report consists of reports from 21 OIC-CERT members

OIC-CERT Guidelines/ Procedures

- Security Frameworks & Models for Organizational Architecture
- A Guideline on Security and Privacy Issues for the Social Network Owner
- Security Guidelines on Industrial Control Systems (**ICS**)
- Guideline on the Internet of Things (IoT)
- Security Software Development Life Cycle (SSDLC) Guideline
- Cloud Security Guideline
- Wireless System Security Guideline
- Cloud Computing Security Guideline
- Promoting the Cybersecurity Industry on a National Level
- The OIC-CERT 5G Security Framework
- Awareness Posters and Presentations

Malware Trend Report

Published 10 Monthly Malware Trend Reports in 2022

OIC-CERT Global Cybersecurity Award 2022

The OIC-CERT Global Cybersecurity Award is an initiative by the OIC-CERT to encourage international collaboration in the cybersecurity domain. The *OIC-CERT Award* recognizes innovative cybersecurity projects from around the world, not bound by country or region, that contribute to the uplifting of the ummah wellness while promoting the digital realm. The theme for year 2022 is *Cyber Resilience for a Prosperous Ummah*

The winner for 2022 is *Project CC Certificate from Qatar NCSA for Huawei NetEngine* by Huawei Technologies Co., Ltd., Qatar

This initiative is in congruence with the OIC-CERT vision to be a leading international cybersecurity platform in having a safer cyber space. This aspiration is achieved by developing cybersecurity capabilities to mitigate cyber threats by leveraging global collaboration

Submissions are open to entities representing the governments, private sector, global and regional institutions, civil society, and academia. The winning submission receives a USD1,000 cash prize. All submissions must be accompanied by the entry form at *www.oic- cert.org/en/globalaward/form*. Submission made to *secretariat@oic-cert.org*

OIC-CERT 5G Security Framework Working Group

With the emergence of the 5G, the members are in the opinion that there is a need to look into the security aspect of this upcoming technology thus the OIC-CERT 5G Security Working Group (**WG**) is formed. This WG is jointly led by Cybersecurity Malaysia, whom is also the OIC-CERT Permanent Secretariat, and Huawei UAE, an OIC-CERT commercial member. Currently, the WG consists of members from 10 countries which are Bangladesh, Brunei Darussalam, Indonesia, Pakistan, Somalia, Tunisia, Malaysia, Morocco, Oman, and the United Arab Emirates

The outcomes of the WG in 2022 were as follows:

- Rollout plan – Egypt, Indonesia, Malaysia, Morocco, Tunisia & UAE
- OIC-CERT 5G Security Framework
    - OIC-CERT 5G Security Framework Part 1: Cybersecurity Repository;
    - OIC-CERT 5G Security Framework Part 2: Baseline Security Technical Specification
    - OIC-CERT 5G Security Framework Part 3: Cross-recognition Assurance Methodology

AZERBAIJAN

Azerbaijan Government CERT (CERT.GOV.AZ)

1. ABOUT CERT.GOV.AZ

1.1. Introduction

CERT.GOV.AZ helps in computer and network security incident handling and provides incident coordination functions for all incidents involving systems and networks located in the state sector of Azerbaijan Republic

RFC-2350 - *http://cert.gov.az/en/pages4/rfc-2350.html*
Promo - *https://www.youtube.com/watch?v=tYqPc-lzd54*

1.2. Host Organisation

- Special State Protection Service of Azerbaijan
- Special Communication & Information Security State Agency
- Azerbaijan Government CERT (CERT.GOV.AZ)

1.3. Establishment

20 Apr 2008

1.4. Resources

Government

1.5. Constituency

Constituency of CERT.GOV.AZ – all networks and the users allocated in state sector of the Azerbaijan Republic

1.6. Summary of Major Activities

Incident Response

CERT.GOV.AZ will assist system administrators in handling the technical and organizational aspects of the incidents. It will provide assistance or advice with respect to the following aspects of the incident management

Incident Triage

- investigating whether indeed an incident occurred
- determining the extent of the incident

Incident Coordination

- determining the initial cause of the incident (the used vulnerability)
- facilitating contact with other sites which may be involved
- making reports to other CERT/ CSIRT teams
- composing announcements to users, when applicable

Incident Resolution

- removing the vulnerability
- liquidation of consequences of incident

- evaluating of possible additional actions considering their cost and risk
- help in evidence collection and data interpretation when needed
- In addition, CERT.GOV.AZ will collect statistics concerning incidents and will notify the community as necessary to assist in protecting against known attacks

Proactive Activities

Information services

CERT.GOV.AZ publishes advisories for events and incidents that are considered of special importance to users in the constituency. Information is disseminated via various channels (web, RSS feeds, mailing lists etc)

Training services

Members of CERT.GOV.AZ periodically hold seminars on various aspects of the information and network security

2. ACTIVITIES AND OPERATIONS

2.1. Events organized by the organization/ agency

- CTF competition dedicated to *The International Cyber Security Day*
- The 1st conference on cyber hygiene called *Safe Digital Environment*
- The 1st Summit of CISOs of the state institutions dedicated to *Safer Internet Day*

The CTF Competition for the International Cyber Security Day

Conference on Cyber Hygiene "Safe Digital Environment"

2.2. Events involvement

- *Fintex Summit* Finance and Technology Conference

"Fintex Summit" Finance & Technology Conference

- *International Cyber Security Days* conference held by the PROSOL company
- *Global Hybrid War and Cyber Security Summit* co-organized by InterProbe and the Association of Cybersecurity Organizations of Azerbaijan

Global Hybrid Warfare & Cyber Security Summit

- Conference organized within the framework of the European Union's Digital Cooperation for Cyber Security and Resilience of Regions in Telc, Czech Republic

CYBER HYGIENE
"Information Security Policy" for the users
Online simulation and test platform – https://kibergigiyena.az
Online trainings to raise information security awareness – https://safavy.az

European Union's Conference in Telc, Czech Republic

- Regional Cybercrime Cooperation Exercise held in Istanbul, Turkey and funded by EU (CyberEast Project)
- National Workshop on cybercrime reporting, use of cyber taxonomies and coordinated Internet Organised Crime Threat Assessment (IOCTA) reporting in Baku, organised under the EU (CyberEast Project)
- OIC-CERT 10th General Meeting & 14th Annual Conference held in Muscat, Oman

PANEL DISCUSSION
OIC-CERT Cybersecurity Industry Development
Regional Cybersecurity Week 2022

The OIC-CERT 14th Annual Conference (Regional Cybersecurity Week 2022)

- *Energy Crisis and Cybersecurity* event held at Azerbaijan State Oil and Industry University

"Energy Crisis & Cybersecurity" held at ASOIU

3. ACHIEVEMENT

- Recorded and handled 480.4M incidents by NGFW, 3.7M malware by centralized endpoint security system, and 223K malicious documents with the special sandbox
- Prevented specifically targeted APT cyberattacks by identifying and

blocking 1,192 Indicator of Compromises (**IOC**s)

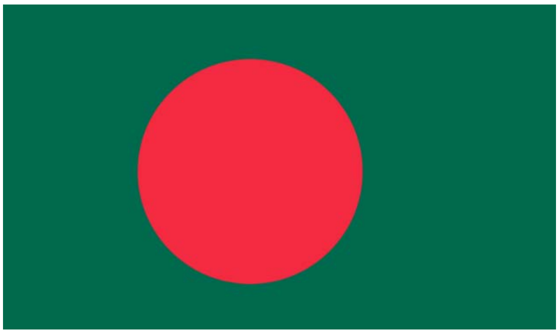
- Blocked 48 impersonated state domains detected by various IT tools
- The largest observed DDoS attack lasted for 8 days (137Gb and 19M rps) and ensured the uninterrupted activity of the state websites
- Processed a total of 27.8M e-mails through the State E-mail Service and blocked 2.2M of them due to their malicious content
- Provided 553 audit/ penetration test for required government bodies
- Received 6383 requests/ tickets from state institutions over the *Electronic Request System* and implemented necessary security measures
- Prepared *the Information Security Policy* and implementation to the 90 state institutions
- Started the cyber hygiene project in which 130 state institutions participated in the test involving 4474 employees where 3990 of them were involved in online training
- Implemented the Azerbaijani language to SIM3 Self Assessment tool

Information Security Journal 2022

- Published *the Information Security* journal for free for government bodies
- Participated in several TV programs to raise awareness
- Discovered the high-risk zero-day vulnerability in the global e-mail service by Ice Warp Inc. (CVE-2022-35115)
- 5,000 desktop calendars were published and distributed to the state institutions for the purpose of awareness as part of the *Information Security Calendar Project* planned for 2023

4. PLANS FOR 2023

- Integrate the OIC-CERT membership and awareness test portals
- Integrate the SIM3 Self Assessment Tool for Security Incident Management Maturity Model into OIC-CERT membership portal
- Continue the *Information Security Calendar Project* to strengthen information security habits and awareness
- Develop the *File Sharing Platform* between the government institutions alternative to *wetransfer* and similar platforms to secure data transfer and maintain within the country's boarders
- Continue collaboration with CERTs internationally



BANGLADESH

Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)

1. ABOUT BGD e GOV CIRT

1.1. Introduction

The Bangladesh Government's Computer Incident Response Team (**BGD e-GOV CIRT**) is acting as the National CERT of Bangladesh (**N-CERT**) currently having the responsibilities of 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 the necessary measures to resolve issues regarding broad cybersecurity ramifications, conducts research & development, and provides guidance on security vulnerabilities. BGD e-GOV CIRT also works with various government units, Critical Information Infrastructures (**CII**), financial organizations, law enforcement agencies, academia & civil society to help to improve the cybersecurity of Bangladesh

1.2. Establishment

The process to establish BGD e-GOV CIRT was started in Nov 2014 and the team started operation in Feb 2016

1.3. Resources

Currently 17 people are working in BGD e-GOV CIRT

1.4. Constituency

The constituency of BGD e-GOV CIRT is all the governmental, semi-governmental, autonomous bodies, ministries, and institutions of Bangladesh. Currently BGD e-GOV CIRT is the N-CERT of Bangladesh with a mandate to serve the country

Celebrating Cybersecurity Week 2022

2. HIGHLIGHTS OF 2022

2.1. Summary of Major Activities

- BGD e-GOV CIRT has successfully organized the National Cyber Drill, Inter University Cyber Drill, and Cyber Drill for Financial organizations
- A total of 522 cybersecurity incidents are registered in the tracking system
- Published the *Ransomware Prevention & First Response Guideline*

- Published the *Digital Forensic Guideline 2.0*
- Published the *Critical Information Infrastructure Guideline Implementation Workbook 1.0*
- Published the *Report on Sectorial Threat Intelligence for Banks July 2022*
- Published the *Cyber Threat Landscape Report 2022*

University Cyber Drill 2022 Host Team

2.2. Achievements

- BGD e-GOV CIRT has successfully participated in OIC-CERT Cybersecurity Drill 2022 and achieved 2nd position
- Participated in the annual FIRST CTF 2022
- Participated in the Annual Asia Pacific Computer Emergency Response Team (**APCERT**) CTF 2022

3. ACTIVITIES AND OPERATIONS

3.1. Events organized by the organization/ agency

- National Cyber Drill 2022
- Inter University Cyber Drill 2022
- Financial Cyber Drill 2022
- Organize a one-day workshop on BGD e-GOV CIRT operations for the ICT Division, Ministry of Post, Telecommunications, and IT
- Organized the stakeholder consultation on Data Protection Act, 2022 (draft)
- Organized a 4-day training program on cybersecurity for the high officials of the ICT Division, Ministry of Post, Telecommunications, and IT

Training on Secure Computer User

- Organized a 4-day training program on Secure Computer User for officials of the Bangladesh Army
- Organized a 3-day training program on the Information Systems Auditing for officials of the Bangladesh Police
- Organized a 3-day training program on advance cybersecurity for personnels from the West Zone Power Distribution Company (**WZPDCL**)
- Organized a 3-day training program on basic cybersecurity for

personnels from the Bangladesh Computer Council

- Organized a 3-day training program on basic cybersecurity for personnels from the Palli Karma-Sahayak Foundation (**PKSF**)

Cybersecurity training for ICT Division Officers

3.2. Events involvement

- National Cyber Drill 2022
- Inter University Cyber Drill 2022
- Financial Cyber Drill 2022
- A one-day workshop on BGD e-GOV CIRT operations for ICT Division, Ministry of Post, Telecommunications, and IT
- Organized a stakeholder consultation on Data Protection Act, 2022 (draft)
- Organized a 4-day training program on cybersecurity for the high officials of the ICT Division, Ministry of Post, Telecommunications, and IT
- Organized a 4-day long training program on Secure Computer User for officials of the Bangladesh Army
- Organized a 3-day long training program on Information Systems Auditing for the officials of the Bangladesh Police
- Organized a 3-day training program on advance cybersecurity for personnels from WZPDCL

Training on Information Systems Auditor

- Organized a 3-day training program on basic cybersecurity for personnels from the Bangladesh Computer Council
- Organized a 3 day long training program on basic cybersecurity for personnels from the PKSF

Award giving ceremony for cyber drill winners

4. ACHIEVEMENT

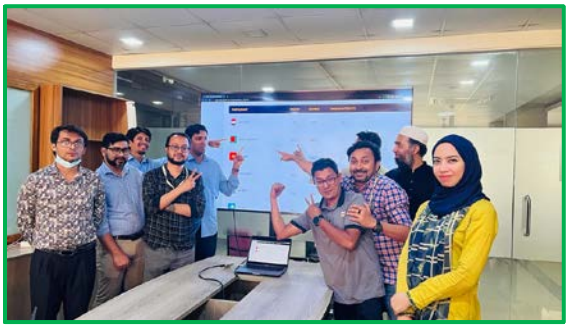
- Provided 40 cyber sensor analysis reports (from Jan - Dec 2022) to multiple CII
- *Cyber Threat Intelligence Report* provided to 60 government and non-government organizations
- 246 cybersecurity advisories and news published on BGD e-GOV CIRT website to inform people about cybersecurity
- Published monthly cybersecurity magazines for the stakeholders

- BGD e-GOV CIRT published *The Cyber Threat Landscape Report 2022*
- In 2022, nine IT security audits were performed
- Provided digital forensics services to a total 7 organizations. Total number of analyzed cases were 11 and total number of investigated artifacts were 36
- Published the *Ransomware Prevention & First Response Guideline*
- Published the *Digital Forensic Guideline 2.0*
- Published the *Critical Information Infrastructure Guideline Implementation Workbook 1.0*
- Published the *Report on Sectorial Threat Intelligence for Banks Jul 2022*
- Published the *Ransomware State of Bangladesh* in Sep 2022
- Published the *Horizon Scanning Report for Bangladesh Telecom Operators* in Q1,2022.

5. 2022 PLANNED ACTIVITIES

- Arrange Cyber Drills for different sectors
- Perform risk-based audit for CIIs and government organizations
- Provide training on ICS in the Public sector
- Perform vulnerability assessment and penetration testing on the financial sectors
- Conduct trainings and workshops on cybersecurity for government organizations
- Provide regular cyber sensor analysis report (intrusion & suspicious activities) to CII where cyber sensors are deployed

Workshop on "Using Social Media to Counter Radicalism" in the presence of the Australian Deputy High Commissioner



Celebrating the success for achieving 2nd place in the OIC-CERT Cyber Drill

Advance Incident Handling training organized by Carnegie Mellon University, USA

Cybersecurity Training in New Delhi

BGD e-GOV CIRT at RSA 2022, USA

National Cyber Drill 2022 Host Team

Cybersecurity training in Dubai, UAE

BRUNEI DARUSSALAM

Brunei Computer Emergency Response Team (BruCERT)

1. ABOUT BruCERT

1.1. Introduction

Cyber Security Brunei (**CSB**) is the national cybersecurity agency of Negara Brunei Darussalam, serving as an administrator that monitors and coordinates national efforts in addressing cybersecurity threats and cyber crime. It operates under the Ministry of Transport and Info communications (**MTIC**), with the Minister of MTIC as Minister-in-charge of Cybersecurity

CSB provides cybersecurity services to the public, private and government sectors in Negara Brunei Darussalam. These cybersecurity services are intended to ensure the following interests

- Increase awareness of cyber threats in the public and private sectors, especially the protection of the CII in Negara Brunei Darussalam
- Improve the ability to respond to cyber incidents through effective cyber crisis management
- Enhance law enforcement capabilities in addressing cyber threats through the services of the National Digital Forensics Laboratory
- Increase public awareness of cyber threats

BruCERT was established in May 2004. It was formed in collaboration with AITI, the Ministry of Communication, to become the nation's first trusted one-stop referral agency in dealing with computer and Internet related security incidents in Negara Brunei Darussalam. It is now under Cyber Security Brunei

BruCERT Services

- 24 x 7 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 emails and telephones as well as mitigating 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 workshops, seminars, and trainings.

- Coordinating with other CERT, Network Service Providers, Security Vendors, Government Agencies as well as other related organization to facilitate the detection, analysis and prevention of security incidents on the internet

1.2. BruCERT Establishment

BruCERT coordinates with the local and international CSIRTs, Network Service Providers, Security Vendors, Law Enforcement Agencies and other related organizations to facilitate the detection, analysis, and prevention of security incidents on the Internet

1.3. BruCERT Workforce

BruCERT currently has a strength of 66 staffs (100% local) where the majority specializes in IT and the rest is administration and technical support. The staff has undergone training on various IT and security modules, such as A+, N+, Linux+, Server+, Security+, SCNP, SCNA, CIW, CEH, CCNA, CISSP, BS7799 Implementer and SANS trainings such as GREM, GCIA, GCIH, GCFA, GPEN, where most of the BruCERT workforce has gained certifications in

1.4. BruCERT Constituents

BruCERT has close relationship with government agencies, a major Internet Service Provider (**ISP**), and various numbers of vendors

Government Ministries and Departments

BruCERT provide security incident response, managed security services and consultancy services to the government agencies. Security trainings such as forensic and awareness trainings were provided by BruCERT in collaboration with other government agencies

E-Government National Centre

E-Government National Centre (**EGNC**) provides IT Services to all the government departments and ministries in Brunei Darussalam. Services such as the IT Central Procurement, Network Central Procurement, Co-location, ONEPASS (a PKI initiative), and Co-hosting are provided by EGNC. BruCERT works closely with EGNC in providing incident response and security monitoring since most of the government equipment reside in 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 Information Technology Protective Security Services (ITPSS), an IT local security company to become the national CERT to deal with security incident response in Brunei collaborating with the Royal Brunei Police Force (**RBPF**) and other law enforcement agencies (**LEA**s)

BruCERT has been collaborating with RBPF and other LEAs to resolve computer-related incidents through the Digital and Mobile Forensic services

Unified National Network

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

1.5. BruCERT Contact

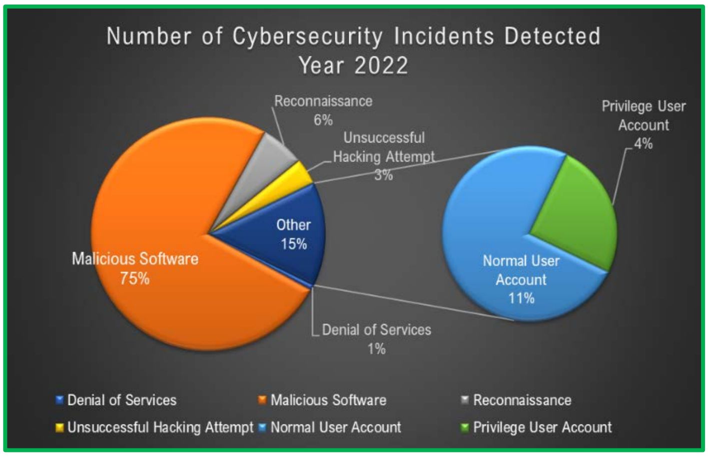
BruCERT welcome reports on computer security related incident. Any computer related security incident can be reported by

Telephone: (673) 2458001
Facsimile: (673) 2458002
Email: cert@brucert.org.bn

2. BRUCERT OPERATION IN 2022

2.1. Incidents Response

For the year 2022, CSB's BruCERT, through the Cyber Watch Centre (CWC), has identified multiple instances of malicious behaviour through the secure monitoring and intelligent sensors, located at the BruCERT constituent systems. Based on these findings, malware infections are the most prevalent form of cyber threat in Brunei Darussalam where some instances involve "*Ransomware*" attacks. The second most common type of incident detected involved attacks on user accounts, including both user and privilege accounts. The following Figure and Table depict the statistics of these security incidents

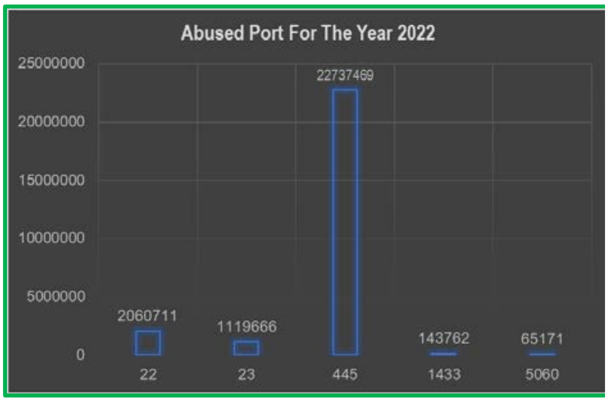


Types of Attacks	Count
Denial of Services	31
Malicious Software	3025
Reconnaissance	244
Unsuccessful Hacking Attempt	146
Normal User Account	434
Privilege User Account	146

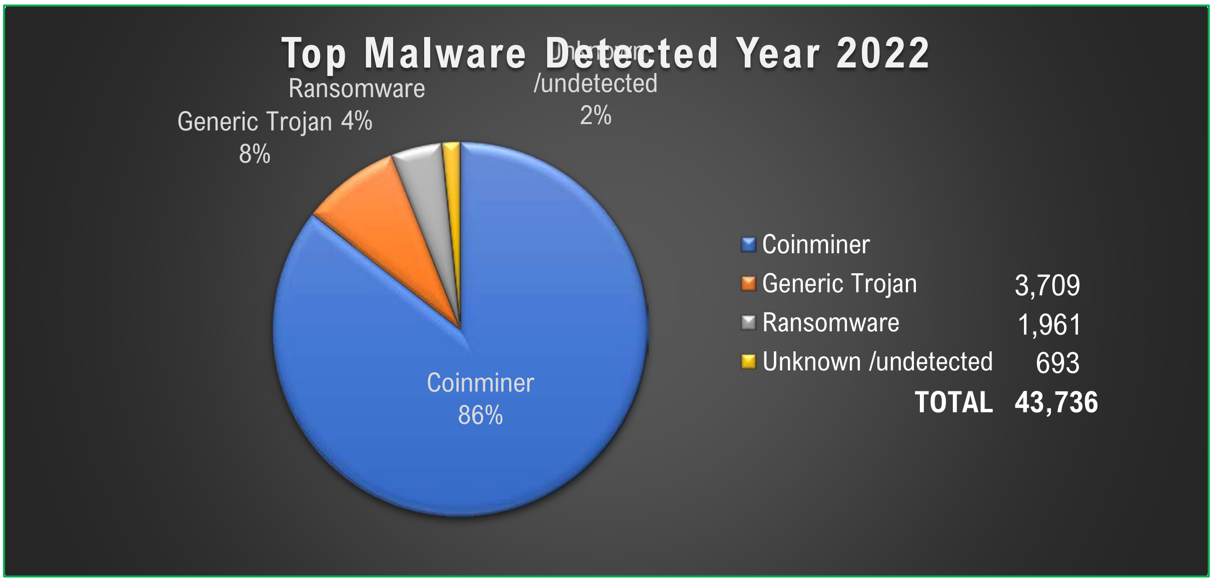
2.2. BRUCERT HONEY POT

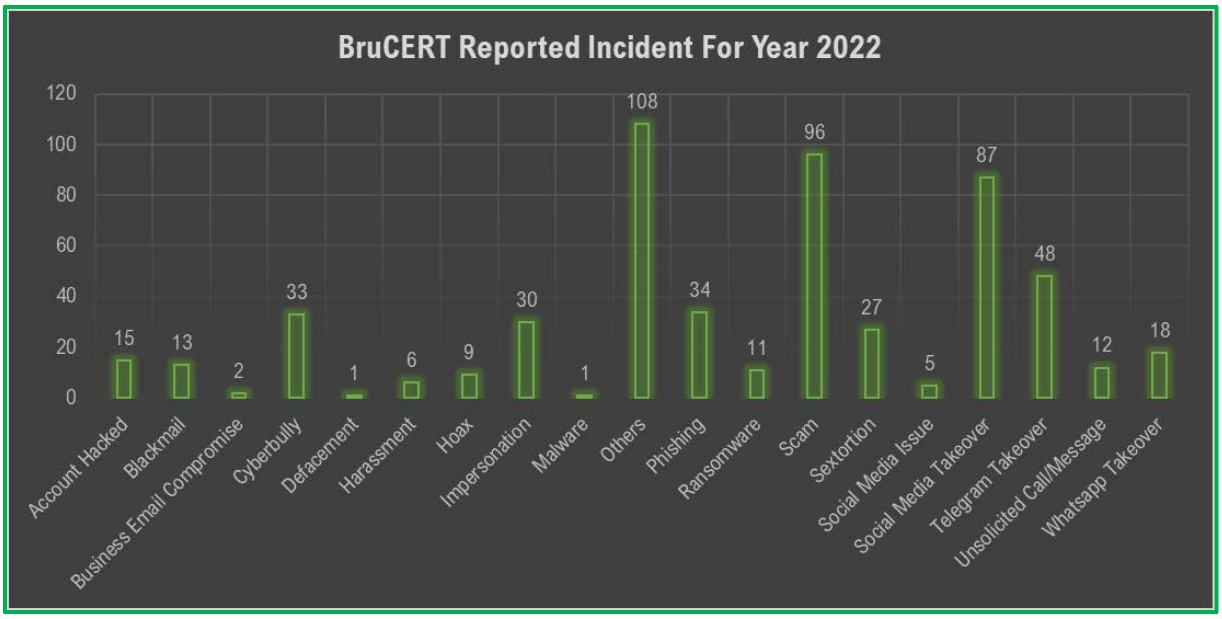
CSB's BruCERT had been deploying a Honey Pot, a test web server to intentionally lure cyber attackers to compromise the server. From the logs extracted from the honey pot, BruCERT had identified that the most abused port number is 445 which is the SAMBA (SMB) followed by port number 22 which is used by Secure Shell Connection (**SSH**) for connectivity

Port No	Count
22	2,060,711
23	1,119,666
445	22,737,469
1433	143,762
5060	65,171



From the honey pot, new variants of malware had been identified as targeting the organizations using port 22 as well as port 445. This is supported by the malware which was captured by BruCERT honey pot shown by the following figure. In another configuration, the BruCERT honey pot managed to capture some of the malware hashes. The following table shows the summary of the most detected malware attacking the honey pot





The year 2022, BruCERT has been receiving incident reports from the general public, including the private sector. In Mar and Aug 2022, BruCERT experienced a significant surge in incident reports received via email and the BruCERT hotline. Most of these reports pertained to "Social Media Issues" and "Scam" activities. The former included instances of social media accounts such as Instagram, Facebook, WhatsApp, and Telegram being successfully compromised or taken over, an increase in such incidents observed in Brunei Darussalam. Compromised social media accounts were often used as part of the scamming activities. Since the outbreak of Covid-19, there has been a rise in scamming activities specifically targeting Bruneians, utilizing local Brunei. Please refer to figure above

3. BRUCERT ACTIVITIES IN 2022

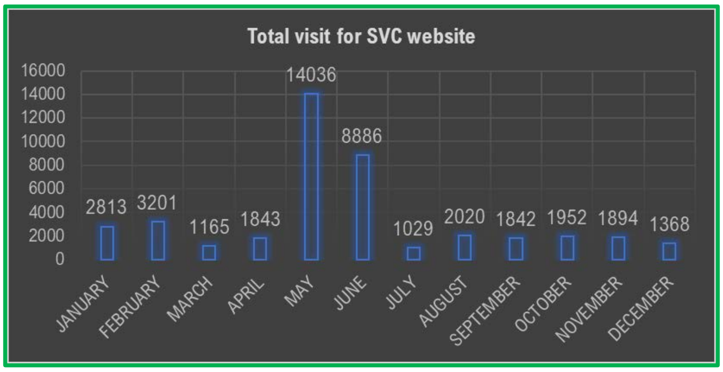
3.1. Seminars/ Conferences/ Meetings/ Visits

BruCERT attended and presented at various seminars, conferences, and meetings on ICT security with some being are done online

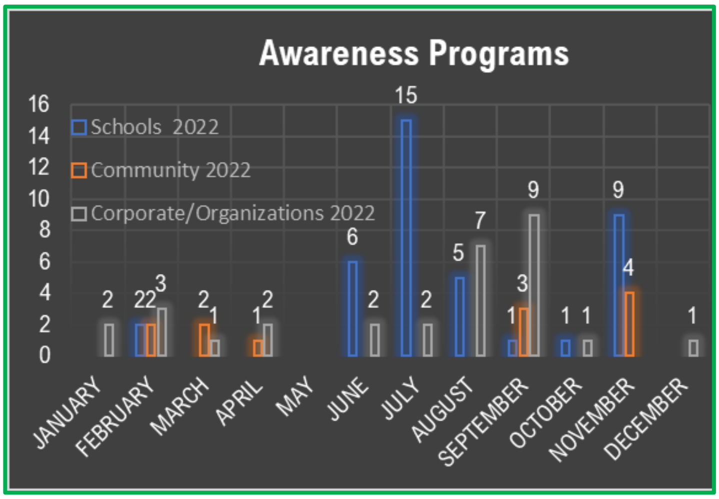
- BruCERT delegates attended the APCERT Annual General Meeting and Annual Conference 2022 conducted online - 18 – 19 Oct 2022
- Three BruCERT delegates attended the OIC-CERT 10th General Meeting & 14th Annual Conference (in conjunction with the 10th Regional Cybersecurity Summit & the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions) which takes place at Muscat, Oman, hosted by OMAN CERT6 - 9 Nov 2022

3.2. Awareness Activities

Throughout 2022, CSB via BruCERT conducted various awareness-raising activities aimed at educating both the general public and public sector about security threats present in the cyber world. The main awareness website is *secureverifyconnect.info*, which received a total of 42,049 website visits. The website experienced the highest traffic in May and Jun, when an advertisement for the BruCERT CTF competition was published



BruCERT awareness talk which was provided to schools, community as well as corporate/ organization also took place almost every month in 2022



INDONESIA

National Cyber & Crypto Agency (NCCA)

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

2022 is a year of revival for more active collaborative activities after the COVID-19 pandemic made everything a vacuum for the last three years. National Cyber & Crypto Agency (**NCCA**) was involved in several face-to-face international programs and collaborations, such as capacity building programs, focus group discussions, working group on cybersecurity policy strategies, and annual activities with international forums

1.2. Achievements

NCCA involves a comprehensive set of measures designed to protect the national digital assets, including computer systems, networks, and sensitive data, from cyber threats. This service includes a range of services such as digital forensic, IT security assessments (**ITSA**), security monitoring, threat hunting & intelligence, and incident response; to help identify, prevent, and respond to security breaches

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

NCCA is a government agency with national responsibility in cybersecurity. It started with the establishment of the Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center (**Id-SIRTII/ CC**) on 4 May 2007 by the Minister of Communication and Information Decree number no 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 operates 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 with NCCA (*Badan Siber dan Sandi Negara* - **BSSN**)

In Apr 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, NCCA

2.2. Establishment

Id-SIRTII/ CC was established on 4 May 2007 and later merged with the LSN to form a new national agency named NCCA, based on the Presidential Decree Number 53 in 2017. NCCA officially started its operation in Apr 2018

2.3. Resources

NCCA, as the new national agency, has several main functions such as detection, monitoring, response & mitigation, cooperation, and as the national security operation centre; covering the areas of government, CII, and digital economy

2.4. Constituency

- Ministries and Government agencies
- LEAs
- National Defence
- CII Operators
- Cybersecurity communities
- ISPs
- Network Access Providers (NAP)
- Local Internet Exchange Operators
- Other Sector CERT/ CSIRT in Indonesia

3. ACTIVITIES AND OPERATION

3.1. Events organized by the organization/ agency

As the Deputy Chair of the OIC-CERT, Indonesia co-lead the OIC-CERT 5th Pillar: Capacity Building, and in 2022 conducted four online capacity building program

- Workshop Network Forensics (with Hands-On)
- Workshop on Incident Management for Decision-Makers
- Managing a **SOC** in Government Sector
- Webinar: "*Promoting Electronic Certificate in Digital Transformation*"

International Cybersecurity Online Work... (Cohost)
BADAN SIBER DAN SANDI NEGARA
wonderful indones

NISC International Cybersecurity Online Workshop & TTX

3.2. Events involvement

On a national scale, 2022 was a special year for Indonesia as the host of G20 Summit in Bali. To support the Indonesian Presidency, NCCA took the role providing cybersecurity and protection during the event

Indonesia also became the host for the Inter-Parliamentary Union (IPU). The 144th General Assembly, and NCCA is responsible for the cybersecurity and protection during the event. The other international event conducted in Indonesia was the ASEAN Para-Games

2022 and NCCA is involved in protecting the event's cyber eco-system

Other than international events, NCCA also involved in national events in 2022, among them are

- National Data Protection Task Force
- Indonesian Independence Day at The Presidential Palace
- Annual Session of the People's Consultative Assembly (MPR)
- National Police Recruitment

3.3. Achievement

In 2022, NCCA received 236 cybersecurity incident reports from various sectors. The monitoring and incident response team also delivered 1,433 cybersecurity notifications. NCCA conducted the ITSA to various national stakeholders, and 1,950 vulnerabilities were found in 457 assessed electronic system. NCCA also collaborated in the digital forensics laboratory services to processed 406 digital evidences in 2022.

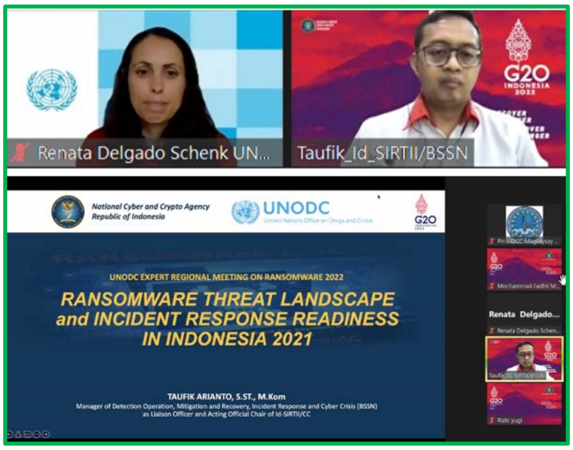
As a national CSIRT, NCCA encouraged the central and regional government, as well as vital infrastructure sectors to establish their own CSIRT. This CSIRT establishment is mandated in the Indonesian Government National Mid-Term Development Program 2020-2024; that at least 121 CSIRT will be established by 2024. NCCA launched 81 sectoral CSIRTs in 2022 which has exceeded the target figure

2023 PLANNED ACTIVITIES

Based on the results of the 2022 OIC-CERT Board election, NCCA once again holds the role of Deputy Chair of the OIC-CERT. NCCA still lead and carry out the Capacity Building pillar, with the plan to conduct several more training activities in the form of webinars and workshops

On a national scale, Indonesia will hold several international events, and NCCA will be involved as the cybersecurity security task force

ITU-UAE "Cyber Protective Shield" Cyber Drill



National Cyber and Crypto Agency
Republic of Indonesia

UNODC
United Nations Office on Drugs and Crime

G20

UNODC EXPERT REGIONAL MEETING ON RANSOMWARE 2022

RANSOMWARE THREAT LANDSCAPE
and INCIDENT RESPONSE READINESS
IN INDONESIA 2021

TAUFIK ARIANTO, S.ST., M.Kom
Manager of Detection Operation, Mitigation and Recovery, Incident Response and Cyber Crisis (BSSN)
as Liaison Officer and Acting Official Chair of Id-SIRTII/CC

United Nations Office on Drugs and Crime (UNODC) bilateral meeting on Ransomware

English Communication for Cybersecurity Professional, MIIS, US Embassy

ASEAN-Japan Policy Meeting & TTX, Japan & Indonesia (Bali - Aug 2022)

Cyber Bootcamp (National Security College, The Australian National University (Jakarta - Aug 2022)

ILEA Computer and Network Intrusion Course

Industrial Control System 301L & Cybersecurity Evaluation Tool by US Embassy

AfricaCERT
Uniting Teams promoting Cybersecurity in Africa
Africa Cyber Security Drill
8-9th September 2022

Africa CERT Annual Cybersecurity Drill 2022

Singapore ACID Drill Test (Singapore Oct 2022)

RCC
المركز العربي الإقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

Arab Drill Test (Saudi Arabia)

Singapore ASCCE Webinar on "UN Cyber Discussions: A Primer"

UNODC Bilateral Meeting on Ransomware (Kuala Lumpur, Malaysia)

24th AJCCBC Cybersecurity Technical Training ASEAN-Japan Cybersecurity Capacity Building Centre (Bangkok, Thailand)

ASEAN-Japan (NISC) Table top exercise (Tokyo, Japan)

FIRST Conference & NatCSIRT Annual Technical Meeting 2022 (Dublin, Ireland)

OIC-CERT General Meeting 2022 (Muscat, Oman)

JORDAN

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

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- Drafting, developing, reviewing, and following up on *Cybersecurity Strategy for the Financial and Banking Sector* (**CSF**) and its programs, work plans, and policies
- Enhancing the sharing of information among the institutions of the banking and financial sectors and the relevant local and international entities
- Raising the competencies of the workers within the banking and financial sectors as well as the employees of the unit

1.2. Achievements

- FinCERT has published the first version of the Financial Sector *Cybersecurity Framework* in Jul 2021
- CSF establishes the sector's cybersecurity baselines, and provide implementation guidelines
- Built upon best practices curated from sector-specific policymakers such as the Federal Financial Institutions Examination Council (FFIEC), leading industry verticals such as the Peripheral Component Interconnect Standard (PCI) and the Society for Worldwide Interbank Financial Telecommunication (**SWIFT**), as well as trusted cybersecurity benchmarks the National Institute of Standards and Technology (NIST) and the International Organization for Standardization/ the International Electrotechnical Commission, (**ISO/IEC**)
- Delivery form - Control Catalogue (What? How?)
- FinCERT established a hub-and-spokes sharing community
- Bi-directional controlled sharing, mandated by the Traffic Light Protocol (TLP)
- FinCERT has structured a sharing platform, leveraging on the Malware Information Sharing Platform (**MISP**) as the interface layer with the financial institutions. Both automated and manual interfaces are supported
- FinCERT published the first version of the computer telephony integration (**CTI**) sharing "*Operational Framework*" with the banks
- Piloted the MISP on Jun 2022
- Since inception, FinCERT has taken up the process of CTI to deliver

sector-centric “finished” intel on a daily basis

- Performing the whole CTI cycle - collection, analysis, validation/ enrichment, and deliver
- CTI Delivery forms (sector-centric)
    - Validated Atomic IOCs
    - Threat intelligence (context-rich)
    - Security Advisories
- Drafting Inherent Risk Profile and Maturity Level Assessment of the banking sector
- Developing Jo-Financial Sector cyber map
- Joining OIC-CERT and FS-ISAC
- In the process of joining TF-CSIRT and FIRST
- Participating in raising the level of International Telecommunication Union - Global Cybersecurity Index (ITU-GCI) of Jordan
- Signing Memorandum of Understanding (**MoU**) with the National Cybersecurity Center in Jordan

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

The Unit of Financial Computer Emergency Response Team (**FinCERT**) seeks to enhance the cybersecurity of the banking and financial sectors and increase their readiness and capabilities to fortify the defences against and respond to cyber risks

2.2. Establishment

The unit was established on 30 Jun 2019 under the umbrella of the Central Bank of Jordan (**CBJ**) to enhance and boost the cybersecurity capabilities of the banking and financial sectors in Jordan

2.3. Resources

The unit is annually funded by the banking sector in Jordan while being hosted on the premise of CBJ

2.4. Constituency

JoFin-CERT is considered a sector centric that serves the financial and banking sectors in Jordan. The targets are banks, exchange companies, payment institutions, and microfinance institutions that are under the supervision of the CBJ. In addition, Jo-FinCERT operates as an Information Sharing and Analysis Centre (**ISAC**) for the above-mentioned entities

3. ACTIVITIES AND OPERATION

3.1. Events organized by the organization/ agency

The unit organized a meeting with the managers of cybersecurity, compliance, and risks from the banking sector on 5 Jul to discuss the latest achievements of the unit and address future plans and initiatives

3.2. Events involvement

Attended the following

- 1st Arab Banking Cyber Security Forum.

- Kaspersky Incident Response Training
- Certified Blockchain Security Professional workshop
- Digital Forensics Examiner training program
- Risk Management Professional Forum conducted by Union of Arab Banking
- Cyber Diplomacy and Governance conducted by the Ministry of Foreign Affairs and Chatham House
- Applying ISO 20022 on SWIFT workshop
- CBL-AFI Virtual Member Training on AFI's Policy Model for Digital Identity and Electronic Know Your Customer (e-KYC) training program
- World Cyber Security Summit - Jordan 2022
- 1st FinCon Jo Forum
- Mandiant GCC Threat Intelligence Briefing
- 6 Quick Wins for Effectual ISRM
- CERES Forum Annual Conference 2022
- "*Defending Against APTs with Adversary Simulations*"
- The 2022 FS-ISAC Europe Summit
- Cyber South
- ISACA 's Annual Forum
- The International Conference on: *Future of Public Administration Global Experiences*
- SWIFT Security Bootcamp
- Building Cyber Resiliency training program conducted by the International Monetary Fund - Middle East Center for Economics and Finance (IMF-CEF)
- MISP Best Practices for Encoding Threat Intelligence
- Visiting Oman Cert (OCERT) from 6 -10 Oct to learn from their experience in information security and cybersecurity and incident response

3.3. Achievement

The unit sponsored the CTF competition held in Jordan organize by NCSC Jordan and Al Hussein Technical University.

4. 2023 PLANNED ACTIVITIES

- Improving the information sharing platform
- Revising the Information Sharing Framework
- Revising Cybersecurity Framework for the Financial Sector in Jordan
- Bank's Maturity Level Assessment
- PSPs' Inherent Risk Assessment
- Financial Cyber Map for Banks
- Cyber Readiness Index
- Brand Protection and Dark Web Monitoring
- Developing awareness programs and training for the banking and financial sectors in Jordan
- Conducting an awareness campaign at the national level

KYRGYZSTAN

Computer Emergency Response Team of Kyrgyz Republic (CERT-KG)

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- develop proposals for the development of a cybersecurity policy
- coordinate activities of organizations and centres for responding to computer incidents (departmental, industry and others) in order to ensure cybersecurity, identify, prevent and suppress computer attacks, while responding to computer incidents
- identification, prevention, and suppression of possible threats and cybersecurity
- making suggestions for improving the legislation of the Kyrgyz Republic in the field of security and cybersecurity
- participation in the development of international treaties of the Kyrgyz Republic in the field of security and cybersecurity
- ensuring the fulfillment of obligations in the field of international relations, participation in which is carried out by the Kyrgyz Republic
- Accomplishment of tasks in accordance with regulatory legal acts of the Kyrgyz Republic

1.2. Achievements

- Assist the citizens in detecting computer incident, CERT-KG launched a web portal "cert.gov.kg ". This portal gave citizens the opportunity to seek help from specialists and get feedback on a computer incident
- Coordination by the Center for Cybersecurity of the State Committee for National Security of the Kyrgyz Republic conducting a number of technical measures to detect computer attacks on the information systems of the state bodies of the Kyrgyz Republic

2. ABOUT THE ORGANIZATION / AGENCY

2.1. Introduction

The Coordination Centre for Ensuring Cybersecurity for the State Committee for National Security of the Kyrgyz Republic (**CERT-KG**) was established to improve the national infrastructure for coordinating and ensuring cybersecurity of the Kyrgyz Republic

2.2. Establishment

CERT-KG was established on 21 May 2020

2.3. Resources

Government

2.4. Constituency

CERT-KG networks, information resources, and users are located in the information space of the Kyrgyz Republic

3. ACTIVITIES AND OPERATION

3.1. Events organized by the organization/ agency

To increase the level of knowledge about cybersecurity during the year, CERT-KG conducted courses and seminars on the topic "*Incident Response*", "*Cyber Hygiene*", and "*Threat Intelligence*" for specialists of the state institutions

3.2. Events involvement

Together with the universities of the Kyrgyz Republic, several seminars were organized for graduates on the trend of cyber threats and the importance of cyber hygiene

4. 2023 PLANNED ACTIVITIES

- Organize and conduct training courses and seminars for employees of the state bodies of the Kyrgyz Republic
- Development of standards in the field of cybersecurity, including requirements for information infrastructure, which must be adhered to
- Conducting a seminar with the participation of the state bodies of the Kyrgyz Republic

LIBYA

Libya Computer Emergency Response Team (Libya-CERT)

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- Participated in the 2nd Libya International Information Technology Forum - Nov 2022
- Held a panel discussion at the Libya International Information Technology Forum - Nov. 2022
- Held a panel discussion on cloud computing security policy for specialists from the cloud computing service providers - Dec. 2022
- Held the International Cybersecurity Awareness Month and campaign - Oct 2022
- Developed the National Information Security & Safety Authority (**NISSA**) fully equipped new digital forensic laboratory and started to conduct laboratory tests
- Assisted NISSA in preparing practical scenarios for the cybersecurity readiness assessment competition (cyber drills). The cyber drill was conducted as an activity in the Libya International Forum for Information Technology
- Participated in the activities of the National Information Technology Day, held at the Corinthia Hotel – Jun 2022
- Participated with NISSA in the Arab Media Week and the activities of Tripoli, Capital of Arab Media 2022, held at the Planetarium, Tripoli - Oct 22-28

1.2. Achievements

- NISSA has enacted The National Cybersecurity Strategy and directed all its constituents to align their strategies with it
- The National Cybersecurity Strategy has been posted on the ITU website
- NISSA is currently working on circulating The National Cybersecurity Strategy to all government and private institutions and sectors
- MoU & Non-Disclosure Agreement (**NDA**) were signed with Moamalat for financial services (the national switch), a key critical national infrastructure of the banking system in Apr 2022 for cooperation in the field of information security
- MoU & NDA were signed with the Ministry of Finance in Jun 2022 for cooperation in the field of information security

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

National Information Safety & Security Authority – NISSA, is the umbrella of the Libya-CERT

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

nissa.gov.ly
www.facebook.com/nissa.libya

2.2. Establishment

NISSA was established by resolution No. (28) issued by the Council of Ministers for the Libyan Interim Government on 22 Jan 2013

2.3. Resources

70 employees.

2.4. Constituency

National: Private & public sectors

3. ACTIVITIES AND OPERATION

3.1. Events organized by the organization/ agency

- NISSA has established and presented a workshop for technical specialists "to present actual scenarios that simulate cyber attacks in the Ministry of Finance and its affiliates
- Conducted several penetration tests and vulnerability assessments for multiple agencies
- Conducted several awareness seminars and workshops throughout the constituency
- Carried out the planned online awareness campaign throughout all NISSA's presence on social media platforms

3.2. Events Involvement

- NISSA has participated in the 4th Cyber Security Innovation Series CSIS event in Tunisia - Sep 2022
- NISSA participated in the activities of the Regional Cyber Security Week 2022. This included the 10th General Meeting and the 14th Annual Conference of the OIC-CERT, which was held in conjunction with the 10th Regional Summit on Cybersecurity and the Regional Symposium for the year 2022. This event included a meeting of the OIC-CERT Board on 6 Nov, followed by other activities, which lasted until the 9 Nov in Muscat, Sultanate of Oman

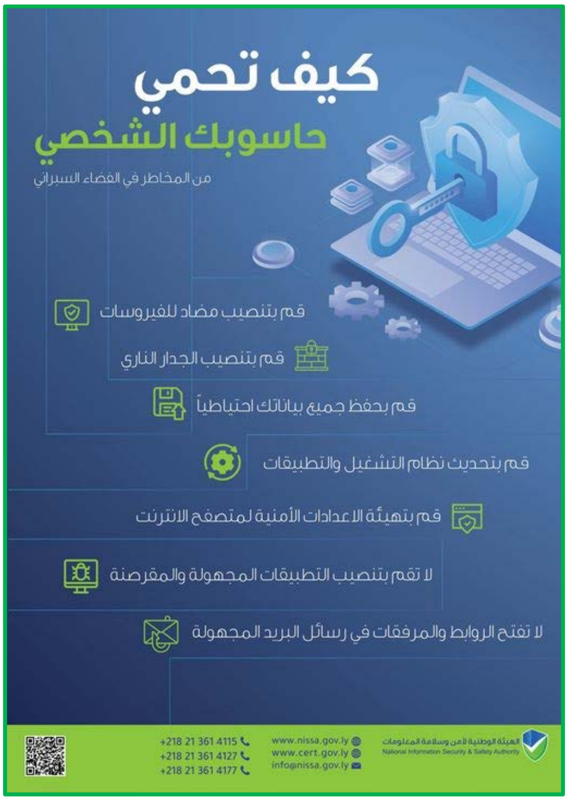
3.3. Achievements

- Significant increase in the reach metrics across all NISSA's online presence
- Several constituents responded positively to NISSA's call to establish a dedicated cybersecurity unit in their hierarchy

4. 2023 PLANNED ACTIVITIES:

- NISSA in the process of joining FIRST – technical requirements under preparation

- NISSA is planning to hold an awareness campaign during the international awareness month - Oct 2023
- A national cyber drill is planned to be organized during 2023 involving most of NISSA's constituency
- In 2023, introductory workshops will be organized on the national strategy for cybersecurity, and many sectors will be targeted in order to align their strategies with The National Cybersecurity Strategy
- NISSA is working on preparing educational programs for cybersecurity in cooperation with the Ministry of Higher Education and the Ministry of Technical Education
- Work on preparing a licensing framework for cybersecurity companies in cooperation with the Ministry of Commerce



كيف تحمي
حاسوبك الشخصي
من المخاطر في الفضاء السبراني

قم بتنصيب مضاد للفيروسات

قم بتنصيب الجدار الناري

قم بحفظ جميع بياناتك احتياطياً

قم بتحديث نظام التشغيل والتطبيقات

قم بتهيئة الاعدادات الأمنية لمتصفح الانترنت

لا تقم بتنصيب التطبيقات المجهولة والمقرصنة

لا تفتح الروابط والمرفقات في رسائل البريد المجهولة

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

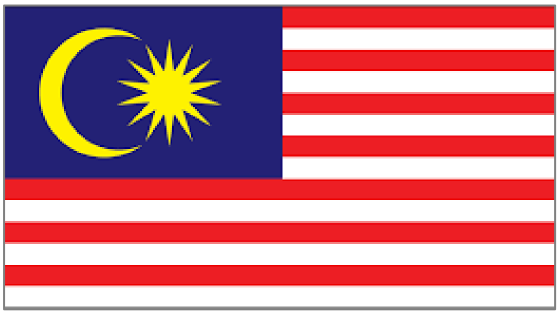
www.nissa.gov.ly
www.cert.gov.ly
info@nissa.gov.ly

+218 21 361 4115
+218 21 361 4127
+218 21 361 4177

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
شهر التوعية بالأمن السيبراني

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
شهر التوعية بالأمن السيبراني

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority



MALAYSIA

CyberSecurity Malaysia

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- Organized 5G Security Framework Workshop - 22 Feb 2022
- Participated in the APRICOT 2022/ APNIC 53 (online) - 21 Feb - 3 Mar 2022
- Organized the Safer Internet Day (SID) 2022: Malaysia Edition in cooperation with BSSN (Indonesia), CSB (Brunei) and the Cyber Security Agency of Singapore (CSA) (online) - 17 Mar 2022
- Participated in the World Police Summit Dubai, United Arab Emirates (**UAE**) - 14-16 Mar 2022
- Participated in the Gulf Information Expo & Conference (**GISEC**) 2022 Dubai, UAE - 21-23 Mar 2022
- Organized a cybersecurity dialogue with industry players at the Royale Chulan Hotel Kuala Lumpur, an initiative under the Cyber Security Collaboration Program (CCP) - 23 Mar 2022
- Participated in Cyber Security for Smart City webinar organized by the Malaysia Smart Cities Alliance Association (MSCA) and the Malaysian Industry-Government Group for High Technology (MiGHT) (online) - 23 Mar 2022
- Participated in the Cybersecurity Innovation Series (**CSIS**) Conference, Egypt Edition Cairo, Egypt - 28 -30 Mar 2022
- Participated in the 21st Annual AusCERT Information Security Conference (online) - 10-13 May 2022
- Organized *Certified Penetration Tester* training (Session 1) under MTCP - 17-24 May 2022
- Participated 34th FIRST Annual Conference, Dublin Ireland - 26 Jun–1 Jul 2022
- Participated in the 4th Cybersecurity Innovation Summit 2022 Tunisia & presented the OIC-CERT 5G Security Framework - 15-16 Sep 2022
- Chaired the APCERT Annual General Meeting (AGM) (online) - 18 Oct 2022
- Organised the Cyber Security Malaysia - Awards, Conference & Exhibition (**CSM-ACE**) 2021 in Cyberjaya, Malaysia - 17-21 Oct 2022
- Participated in the OIC-CERT Cyber Drill with the theme *The Rapid Evolving of Cyber Threats Landscape in Parallel with Innovation in Cybersecurity Industry* - 7 Nov 2022
- Organised the OIC-CERT 10th General Meeting & 14th Annual Conference 2022 with the theme "*Cybersecurity Innovation and Industry Development*", Muscat, Sultanate of Oman - 6-9 Nov 2022

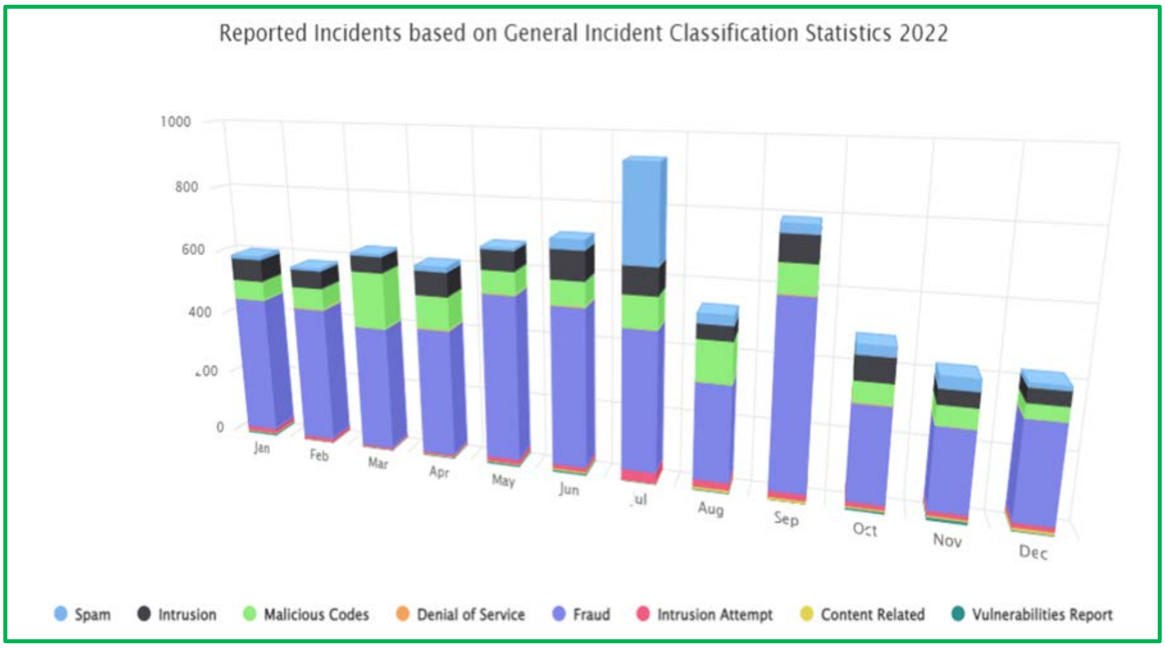
1.2. Achievements

Cyber999 Cyber Incident Reference Centre

CyberSecurity Malaysia receives reports from various parties within the constituency such as home users, private sectors, government sectors, and security teams from abroad (foreign CERTs), Special Interest Groups, as well as through the internal proactive monitoring by CyberSecurity Malaysia.

CyberSecurity Malaysia through MyCERT had proactively produced 56 advisories and 20 alerts to inform the constituency on issues relating to cybersecurity. The specific list of the advisories, alerts and summary reports can be viewed at *https://www.mycert.org.my/portal/advisories*

Most of the incidents reported were related to fraud and followed by the intrusion. The following figure shows the reported incidents managed by MyCERT



Further information on incidents reported to CyberSecurity Malaysia can be viewed at *https://www.mycert.org.my/portal/statistics-2022*

Cyber Threat Research Centre (CTRC)

The centre operates a distributed research network for analysing malware and cybersecurity threats. The centre had also established collaboration with trusted parties and researchers in sharing threat research information

Other activities by the centre includes

- Conducting research and development work in mitigating malware threats
- Producing advisories on the latest threats
- Threat monitoring via the distributed honeynet project

- Partnership with universities, other CERT's, and international organisations

Lebahnet Project

LebahNET is a Honeypot distributed system where a collection of honeypots is used to study on how the exploits functioned as well as to collect malware binaries. Honeypots are computer software mechanism 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/*

The URLs of the LebahNET project are

- the LebahNET portal at *https://dashboard.honeynet.org.my/*
- the Kibana portal at *https://es.honeynet.org.my/s/public/app/canvas#/workpad/workpad-5e83726d-0125-4bfd-a8e9-88b6e844ce24/page/1*

  by using guest authentication

  Username: guest

  Password: guest2021!

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

CyberSecurity Malaysia is the national cybersecurity specialist agency under the Ministry of Communications and Multimedia Malaysia having the vision of being a globally recognised National Cyber Security and Specialist Centre. Some of the services provided are

Cybersecurity Emergency Services

- Security Incident Handling
- Digital Forensic

Security Quality Management Services

- Security Assurance
- Information Security Certification Body

Cybersecurity Professional Development and Outreach

- Info Security Professional Development
- Outreach

Cybersecurity Strategic Engagement and Research

- Government and International Engagement
- Strategic Research

Industry and Research Development

2.2. 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 2018, with the restructuring of the government administration, CyberSecurity Malaysia was transferred to the Ministry of Communications and Multimedia Malaysia which later became the Ministry of Communications and Digital.

CyberSecurity Malaysia is committed in 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 the cyberspace

2.3. Cybersecurity Incident Management

CyberSecurity Malaysia managed security incidents through MyCERT, a department within CyberSecurity Malaysia. The agency is a leading point of reference for the Malaysian Internet community when faced with cybersecurity incidents. MyCERT facilitates the mitigation of cyber threats for Malaysia's Internet users particularly on cyber intrusion, identity theft, malware infection, and cyber harassment, among others

MyCERT operates the Cyber999 Cyber Incident Reference Centre and Cyber Threat Research Centre that provide technical support for incident handling, malware advisories, and research, respectively. More information about MyCERT can be found at *https://www.mycert.org.my/*

- Cyber999 Cyber Incident Reference Centre

MyCERT operates the Cyber999 Cyber Incident Reference Centre, providing an avenue for Internet users and organisations, to report or escalate cybersecurity incidents that threatens personal or organisational security, safety, or privacy. Channels for reporting cyber abuses and grievances to MyCERT's Cyber999 cyber incidents reference centre are available at MyCERT's website *https://www.mycert.org.my/portal*

MyCERT's Cyber999 cyber incident reference centre, has responded to 7,292 incidents in 2022 and most being malicious codes and online fraud

- Cyber Threat Research Centre

Another valuable service from MyCERT is the malware research with the establishment of the Cyber Threat Research Centre. The centre has been in operation since December 2009 and functions as a research network for analysing malware and cybersecurity threats. The centre conducts research and development work for mitigating malware threats, producing advisories, monitoring threats, and collaborating with other malware research entities

2.4. Resources

CyberSecurity Malaysia services include predictive, detective, responsive, and corrective capabilities as well as recovery

This agency provides technical solutions and services to the Government of Malaysia among which are LEAs, ministries, regulatory bodies and government agencies, private organisations, and the Internet users in Malaysia

CyberSecurity Malaysia's scope of specialised cybersecurity services are as follows

- Cyber Security Responsive Services
- Cyber Security Proactive Services
- Outreach and Capacity Building
- Strategic Study and Engagement
- Industry and Research Development

2.5. Constituency

CyberSecurity Malaysia's constituency is the Internet users of Malaysia. Cybersecurity incidents within Malaysia that are reported either by the Malaysian public or international organisations will be resolved by assisting the complainants with technical matters. If an incident involves international cooperation, CyberSecurity Malaysia will request trusted parties in the country or constituency, of which the origin of the case, to assist in resolving the security issues

3. ACTIVITIES AND OPERATION

3.1. Events Organized by the Organization/ Agency

Trainings

Several workshops or hands-on training were conducted by CyberSecurity Malaysia in 2022

- Certified Penetration Tester training and certification under the MTCP - 17-20 & 23-26 May 2022, 14-17 & 20-21 Jun 2022

  This training aims to raise awareness and provide exposure to participants on the importance of cybersecurity. In addition, participants sit for the '*Certified Penetration Tester*' examination to obtain professional certification

- Cybersecurity & Ethics Webinar: This training provides exposure to the police on digital evidence and cryptocurrency handling procedures while at the same time strengthening cooperation between the two parties - 1 Jul 2022
- Examination and Analysis of Electronic Evidence Online Training: This training program assess the participants' level of knowledge on various aspects of electronic evidence as well as improve their skills in handling cases related to electronic evidence - 5 Jul 2022
- Cyber Crime Prosecution Course: This course exposed participants to the prosecution of cybercrime cases in Malaysia, in addition to improving their knowledge and skills on investigation techniques - 3 Aug 2022
- "*Digital Security Professional Development & Lifelong Learning Program*" under the MTCP: A national program focusing on enhancing relevant cybersecurity capabilities for participating countries and provides validation for participants who have demonstrated capabilities in cybersecurity capacity building through desktop exercises and examination - 23-26 & 29-30 Aug 2022

- The Digital Evidence and Cryptocurrency Handling Procedures Course: This training to provide exposure for the police on digital evidence and cryptocurrency handling procedures and strengthen cooperation between the two parties - 25 Aug 2022

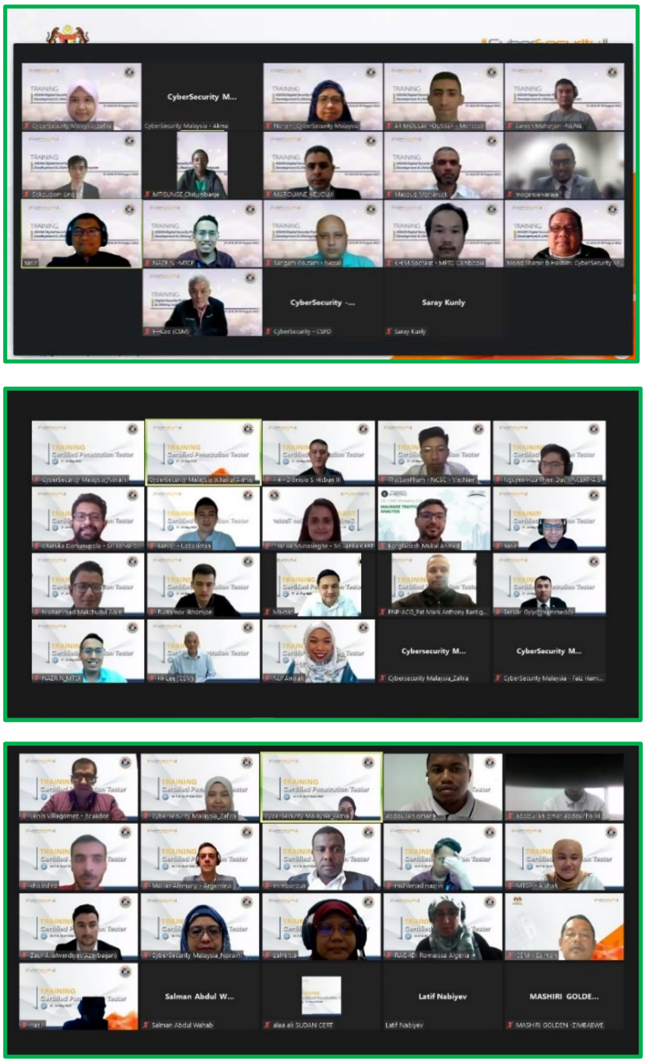
The Malaysian Technical Cooperation Programme

CyberSecurity Malaysia in collaboration with the Ministry of Foreign Affairs Malaysia successfully organised 3 training sessions entitled "*Certified Penetration Tester*" on 17-24 May and 14-21 Jun 2022, and "*ASEAN Digital Security for Lifelong Learning Program*" from 23-30 Aug 2022 under the MTCP

The MTCP was formulated based on the belief that the development of a country depends on the quality of its human resources. Developing capabilities in cybersecurity area is essential for developing countries to ensure less dependency on foreign countries and at the same time nurture self-reliance to protect their digital citizens

In relation to this, the training programme leverages on state-of-the-art cybersecurity knowledge from domain experts and experience practitioners. Certified Penetration Tester is a hands-on training and certification programmes that enable the participants to handle the vulnerability assessment and penetration test for their clients

33 participants from the 20 countries attended the trainings



The MTCP Opening Ceremony

The OIC-CERT 5G Security Working Group

In 2022, the WG has done several rollout plan activities in Malaysia, Egypt, Indonesia, Tunisia, and UAE. Besides that, the WG has developed the following documents

- The OIC-CERT 5G Security Framework Part 1: Cybersecurity Repository

- The OIC-CERT 5G Security Framework Part 2: Baseline Security Technical Specification
- The OIC-CERT 5G Security Framework Part 3: Cross-recognition Assurance Methodology.

Framework Roll Out Activities in Kuala Lumpur & UAE

3.2. Events Involvement

Cyber Drills

CyberSecurity Malaysia, participated in three (3) international cyber drills in 2022 namely the APCERT Drill, ACID Drill, and the OIC-CERT Drill.

The OIC-CERT 10th General Meeting & 14th Annual Conference

This annual event was conducted physically, after 2 years being online. On 7 Nov, the OIC-CERT 10th General Meeting was held in Muscat, Oman with the attendance of 15 OIC-CERT Full members. The new Board for the term 2023-2024 was elected during the meeting. The new Board consist of the following

- Chair: Oman
- Deputy Chair: Indonesia & UAE
- Secretariat: Malaysia
- Board members: Azerbaijan, Brunei, and Egypt

The OIC-CERT Annual Conference hosted by the Oman CERT and ITU-Arab Regional Cybersecurity Centre (**ITU-ARCC**) was held 8 - 9 Nov 2022 in Muscat, Oman. The theme of the event is "*Cybersecurity Innovation and Industry Development*". Dato' Ts. Dr. Amirudin Abdul Wahab FASc was one of the speakers for Panel Discussion 2: "*OIC-CERT Cybersecurity Industry Development*"

OIC-CERT Members attending the OIC-CERT 10th General Meeting, Muscat,Oman

Presentations

CyberSecurity Malaysia had been invited to give presentations and talks at international conferences and seminars among them

- Dato' Ts. Dr. Amirudin was invited to become a panelist for the forum entitled "*Cross-border partnerships to defend the cyberspace: Mitigating next-generation cybercrime through technology and intelligence*" at the International Conference World Police Summit for law enforcement and professionals during the Dubai Expo 2020, UAE - 14 – 16 Mar 2022
- Dato' Ts. Dr. Haji Amirudin is a panelist for the forum entitled "*Speed challenges on cyber and the Future of Policing*" at the INTERPOL Young Global Police Leaders Program (**YGPL**) during the Dubai Expo 2020, UAE - 17 Mar 2022
- Ts. Mohd Shamir is a presenter at the opening address of the Telecom Cybersecurity Program during GiSEC 2022 Dubai, UAE entitled "*The OIC-CERT 5G Security Framework- Building a coordinated effort to harness deep tech for digital transformation*" - 21 Mar 2022
- Ts. Mohd Shamir is a speaker at the CSIS - Egypt Edition, Cairo, Egypt entitled "*The OIC-CERT 5G Security Framework- Building a coordinated effort to harness deep tech for digital transformation*" - 28 – 29 Mar 2022
- Ts. Mohd Shamir is a moderator at the CSIS – Tunisia Chapter, Tunis, Tunisia entitled "*Addressing the Shortage in Talent as Cyber Threats Continue to Evolve Rapidly*" - 16 Sep 2022
- Sharifah Roziah is a speaker at the APCERT Closed Conference 2022 entitled "*How Security Incidents are Responded and Handled Across Different National CSIRTs: Findings from an Online Survey*" - 19 Oct 2022

Research Papers

CyberSecurity Malaysia actively contributed research papers to journals and conference proceedings. Following are some of the papers published

- Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework – IEEE
- RENTAKA: A Novel Machine Learning Framework for Crypto-Ransomware Pre-Encryption Detection – IJACSA
- A Proposal in Having a Cyber Resilience Strategy For The Critical National Information Infrastructure Sectors in Malaysia – OIC-CERT
- Incident Response Practices Across National CSIRTS: Results from an Online Survey – OIC-CERT
- A Theoretical Comparative Analysis of DNA Techniques Used in DNA Based Cryptography – UMT
- SPA on Modular Multiplication in Rabin-p KEM - MSCR
- How National CSIRTs Operate: Personal Observations and Opinions from MyCERT – IEEE
- GSMA 5G CyberSecurity Knowledgebase & NESAS Whitepaper - Huawei Technologies Malaysia
- Analysis of Permutation Functions for Lightweight Block Cipher Design - Society for Cryptology Research - MSCR
- LAO-3D: A Symmetric Lightweight Block Cipher Based on 3D Permutation for Mobile Encryption Application – MDPI
- Statistical Analysis of 3D RECTANGLE Encryption Algorithm - Research World International
- Crypto-Ransomware Early Detection Framework Using Machine Learning Approach – Academia Industry Networks
- How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study – Henry Stewart Publications

Social Media

In 2022, CyberSecurity Malaysia received continuous invitations to speak in cybersecurity events at the local radio and television stations. CyberSecurity Malaysia also actively disseminates cybersecurity concerns through social media such as the Facebook and Twitter, which as of now the Facebook Page has about 56,243 followers and the CyberSecurity Malaysia Twitter has 7,638 followers

4. INTERNATIONAL COLLABORATION

The Malaysia Cybersecurity Strategy 2020 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

4.1. 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

- The National Institute for Research and Development in Informatics – ICI Bucharest
- The Association of Information Security Professionals, Singapore
- The Ministry of Information Communication Technology and Postal Services, Republic of South Sudan
- The National Revenue Authority (NRA), Republic of South Sudan
- Courtesy visit by EUROCHAM Malaysia
- The Republic of Botswana
- Presidential Advisor of International Relations & Program Coordinator, Somalia
- Cyber Security Brunei

4.2. International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia

- The Permanent Secretariat of the Organization of Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**), where the major role is to undertake daily operations and facilitate member activities
- The co-lead for the Capacity Building Initiatives Pillar of the OIC-CERT
- Co-lead the OIC-CERT 5G Security Working Group with the objective of developing a security framework to be adopted by OIC member countries
- The Chair of the APCERT
- Member of the FIRST
- The Convenor for the APCERT Malware Mitigation Working Group – addressing malware infection among Internet users and cyber threat general issues. The main objectives are to provide an overview of the cyber threats landscape by doing collaborative research to mitigate the cyber threats and sharing regular reports or data on malware attacks and focus on the impact analysis and remedial action

5. FUTURE PLANS

CyberSecurity Malaysia strives to improve the service capabilities and encourage 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 proactively be intensified

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 MoUs and agreements

CyberSecurity Malaysia in conjunction with the Aerosea Exhibitions Sdn. Bhd will be organizing an international event known as the Cyber Digital Services, Defence and Security Asia (**CyberDSA'23**). This event is scheduled to take place on 15 – 17 Aug 2023, at the Kuala Lumpur Convention Centre. Concurrently, with this prestigious show, the CSM-ACE and Sibersiaga will be held. The CSM-ACE which is an annual event providing awareness, trainings, and awards to information security professionals, and the National ICT Security Discourse to boost the cybersecurity awareness among the youth. 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 CSIRT by providing consultation and assistance especially in becoming members to the international security communities such as the APCERT, FIRST and OIC-CERT

FNS (M) Sdn Bhd

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- Promote Passwordless Blockchain Secure Authentication (BSA) solution globally through partners and customers in Asia Pacific, Middle East, Europe, and North America

BSA
PASSWORDLESS
Go Passwordless with BSA
"Making the world safer with Blockchain Secure Authentication"
SECURE . FAST . CONVENIENT
FNS (M) SDN.BHD.
FEASIBLE NETWORK SYSTEM

- Awareness to regional and global market via ITU-T SG17, OIC-CERT, and SFF 2022
- Participated in global events as speaker and exhibitor (e.g., Bank Negara Malaysia, MyFintech, XCION, WTSA-20, SFF 2022)

- Contributed in the Technical Code development specifically for the Security, Trust, and Privacy Working Group (STP WG) of Malaysian Technical Standards Forum Bhd (MTSFB)
- Contributed for a new work item proposal to Q14/17 of ITU-T SG17 on "*Access security distributed ledger technology* (DLT) *system*" and presented BSA in ITU-T DLT Workshop in Geneva, Switzerland
- Presented BSA at Tutorial Session ITU-T SG17 Security meeting in Geneva, Switzerland
- Established a Blockchain Security Working Group in OIC-CERT to identify security aspects of DLT systems and to explore use cases of DLT systems in securing digital services
- Associate Member of the Singapore Fintech Association (SFA) from 15 December 2022

1.2. Achievements

- Received product security certification CCRA EAL2 for G-CCS (BSA) from CyberSecurity Malaysia – 12 Aug 2022
- Received OIC-CERT Global Cybersecurity World 2021 award during the ITU-T ARCC Regional Cybersecurity Week 2022 in Muscat, Oman – 8 Nov 2022
- ITU-T TSB has approved FNS (M) Sdn Bhd as the Associate Member of ITU-T SG17 Security - 24 Oct 2022
- Shortlisted as Top 20 on Category 5, Action Line Building Confidence and Security in Use of ICTs for "*Go Passwordless with Blockchain Secure Authentication*" to ITU WSIS Prizes 2023

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

FNS (M) SDN BHD or FNSM, a company incorporated in Malaysia, having the registered address at Suite 5.01, Level 5, Menara LGB, No. 1, Jalan Wan Kadir, Taman Tun Dr Ismail, 60000 Kuala Lumpur, Malaysia. FNSM is a wholly owned subsidiary of FNS VALUE CO. LTD. or FNSV, a company organized and existing under the laws of the Republic of Korea, having its principal office at (Sangam dong, Nuri Dream Square 7th floor) 396, World Cup buk-ro, Mapo-gu, Seoul, Republic of Korea

The vision is "*Making the world a safer place with passwordless blockchain secure authentication*" with Zero-Trust Access Security

BSA is the global first patented passwordless blockchain secure authentication services that replaces User ID and Password to Passwordless BSA MFA to ensure security, privacy, confidentiality, integrity and authenticity of digital services

Website: *https://fnsmalaysia.com/*

LinkedIn:
https://www.linkedin.com/company/fns-m-sdn-bhd/

2.2. Establishment

FNS (M) Sdn Bhd was established in Feb 2020 to represent FNSV in Asia Pacific, Middle East, Europe, and North America

2.3. Resources

14 employees of management, sales and marketing, product development, engineering, and administration

2.4. Constituency

Sector: Government, BFSI, Education, and Healthcare

3. ACTIVITIES AND OPERATION

3.1. Events organized by the organization/ agency

- Hosted Raya Aidilfitri Open House and Housewarming - 16 May 2022

3.2. Events involvement

- Virtual BNM MyFintech as exhibitor and speaker - 24 - 28 Jan 2022
- WTSA-20 as exhibitor and speaker in Geneva, Switzerland - 28 Feb – 4 Mar 2022
- MTSFB STP WG Workshop as industry experts in Bangi, Selangor - 23 - 25 Mar 2022
- Virtual XCION as speaker - 7 Apr 2022
- Virtual World Bank Webinar as speaker - 10 May 2022
- Indonesia business meeting in Jakarta, Indonesia - 22 - 26 May 2022
- TM ONE Tech Update for Ministry of Education as speaker in Pulau Redang, Terengganu - 10 - 12 Jun 2022
- Virtual Innov8tif Webinar as speaker - 20 Jul 2022
- SG17 meeting in Geneva, Switzerland - 23 Aug - 2 Sep 2022
- XCION as observer and participant in Bali, Indonesia - 21 - 23 Sep 2022
- PDRM Tech Update as speaker in Port Dickson, Negeri Sembilan - 13 Oct 2022
- SFF 2022 as exhibitor at Singapore Expo, Singapore - 1 - 4 Nov 2022
- OIC-CERT as speaker at OIC-CERT AGM in Muscat, Oman - 7 Nov 2022

3.3. Achievement

- Established business partners and customers thru participated events/ exhibitions/ webinars in Asia Pacific, Middle East, Europe, and North America
- Received product security certification CCRA EAL2 for G-CCS (BSA) from CyberSecurity Malaysia - 12 Aug 2022
- Received the OIC-CERT Global Cybersecurity 2021 Award during the ITU-T ARCC Regional Cybersecurity Week 2022 in Muscat, Oman - 8 Nov 2022
- ITU-T TSB has approved FNS (M) Sdn Bhd as an Associate Member of ITU-T SG17 Security - 24 Oct 2022
- Shortlisted as Top 20 on Category 5, Action Line Building Confidence and

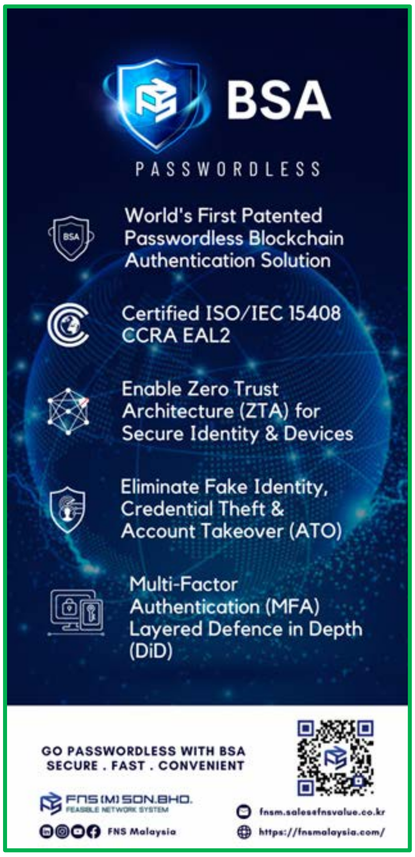
Security in Use of ICTs for "*Go Passwordless with Blockchain Secure Authentication*" to ITU WSIS Prizes 2023

- Contributed in 3 draft Technical Codes of MTSFB STP WG for registration under CMA 1998 by the Malaysian Communications and Multimedia Commission (MCMC)

4. 2023 PLANNED ACTIVITIES

- Continue promoting Passwordless BSA solution globally thru its partners and customers in Asia Pacific, Middle East, Europe, and North America
- Establish Blockchain Security WG and promote the adoption of Passwordless BSA to OIC-CERT members
- Organise BSA Summit 2023 to promote Passwordless BSA solution and to recognize FNSM business partners and customers
- Participate in regional and global events (e.g., OIC-CERT, MCION, WCIT 2023, CyberDSA 2023, SFF 2023) as speaker and exhibitor
- Continue participation in the Technical Codes development activities of MTSFB STP WG, APT ASTAP and ITU-T SG17

1ITU WTSA-20, Geneva 28 Feb - 4Mar 2022



BSA

PASSWORDLESS

World's First Patented Passwordless Blockchain Authentication Solution

Certified ISO/IEC 15408 CCRA EAL2

Enable Zero Trust Architecture (ZTA) for Secure Identity & Devices

Eliminate Fake Identity, Credential Theft & Account Takeover (ATO)

Multi-Factor Authentication (MFA) Layered Defence in Depth (DiD)

GO PASSWORDLESS WITH BSA
SECURE . FAST . CONVENIENT

FNS (M) SDN.BHD.
FEASIBLE NETWORK SYSTEM

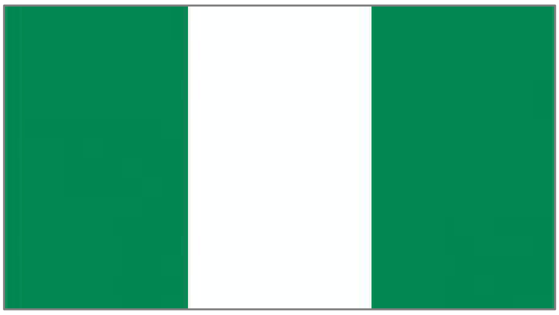
fnsm.sales@fnsvalue.co.kr

FNS Malaysia

https://fnsmalaysia.com/

OIC-CERT
10th OIC-CERT GENERAL MEETING & 14th ANNUAL CONFERENCE 2022
Cybersecurity Innovation and Industry Development
6 - 9 November 2022 | Kempinski Hotel Muscat, Sultanate of Oman
fnsvalue
FNS (M) SDN.BHD.
FNS Malaysia
https://fnsmalaysia.com/

10th OIC-CERT AGM, Oman



NIGERIA

Consultancy Support Services (CS2) Limited

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

Nigerian Civil Aviation Authority (NCAA) Digital Assets and Inventory successfully completed with Provision of Security Audit of a VPN Solution Device for Federal Roads Safety Corps (2022). The 2nd African Cybersecurity Drill 2022; Organisation of Islamic Cooperation (OIC) Computer Emergency Response Team (OIC CERT) Cyber Drill (2022)

1.2. Achievements

- Completed the Digital Assets and Inventory of Nigerian Civil Aviation Authority (NCAA), Aviation Regulatory Agency in Federal Republic of Nigeria
- Completed the Security Audit of a VPN Solution Device of Federal Road Safety Corps (FRSC)
- Supported the Department of Cybersecurity of the Admiralty University of Nigeria, Delta State, Nigeria is obtaining re-accreditation of the department and its cyber-forensics teaching, learning and research activities
- Continue to Chair and support the Nigeria Computer Society (NCS) Cybersecurity Advisory Group
- Facilitated training activities including the Executive Registration Programme (ERP) of the Computer Professionals Registration Council of Nigeria (CPrN) (2022)

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

The Consultancy Support Services Limited (CS2) is a Cybersecurity, e-Library and ICT Policy Consultancy Firm

2.2. Establishment

Consultancy Support Services Limited was incorporated on 13 Feb 2002

2.3. Resources

Cybersecurity Specialist, Library and Information Management Specialist, Information Management and Systems Networking, Computer Programming & Enterprising Management, Digitization, Archiving & Digital Libraries, Computer Forensics & Cyber Security, Digital Library, and Information Technology Infrastructure

2.4. Constituency

Public and Private sectors as well as Academia, Media, and Non-Governmental Organisations in Nigeria, African and across the globe

3. ACTIVITIES AND OPERATION

3.1. Events organized by the organization/ agency

The 2nd African Cybersecurity Drill (2022) and Organisation of Islamic Cooperation (OIC) Computer Emergency Response Team (OIC-CERT) Cyber Drill (2022)

3.2. Events involvement

- Osun State University Security, Insecurity and World Peace: The Humanitarian Perspectives – 1 - 3 Mar 2022
- AUDA-NEPAD & Ghanaian Cyber Security Agency, Accra, Ghanian – 16 – 18 Mar 2022
- ASEAN Norms Implementation Workshop – 23 Mar 2022
- Regional Workshop on Cybersecurity and Digitization, National Open University of Nigeria – 29 Mar 2022
- CySec African Summit Opening Panel: *Security Beyond Borders Cyber Diplomacy for a Secure Future* – 6 - 7 Apr 2022
- Defense Headquarters Development of Cyber Warriors – 13 Apr 2022
- Workshop Faculty on Cyber Threat, Detection and Mitigation for Financial Stability for Central Bank of Nigeria Staff - 19 Apr 2022
- Nigeria Data Protection Bureau (NDPB) Working Group Chair – 25 Apr 2022
- ECOWAS-G7 GFCE Workshop Cyber Africa Forum; "*Digital sovereignty and data protection: Levers of Economic Growth for the African Continent*" – 9 - 10 May 2022
- Gate Foundation: Digital Research Discussion, Transcorp Hilton Abuja – 18 May 2022
- CYSEC NG 2022: "*Emerging Cyberthreats: Landscape and Defense*", Keynote Speaker – 25 May 2022
- FITC Leadership Programme on "*Effective Board Leadership and Performance in a Disruptive VUCA Environment: Aligning People, Processes and Innovations*" Dubai. Lead Discussion - 7 -11 Jun 2022
- Resource Person Cyber Security Expert Association of Nigeria (CSEAN) "*Cyber Governance and Security; Lessons from across the globe*" at the Cyber Secure Nigeria 2022 conference - 21 – 22 Jun 2022
- CyFrica Summit 2022: "*Strengthening Africa's Digital Ecosystem: Implementing Effective Cybersecurity Framework*", Kenya VIP Speaker – 28 - 29 Jun 2022
- African School on Internet Governance (AfriSIG), Malawi – 19 - 21 Jul 2022

- Lecture on Cyber Warfare and Air Power for Air Force War College, Makurdi – 12 Aug 2022
- Participated in the United Nations AdHoc Committee to Elaborate a Comprehensive International Convention on Countering the use of ICT for Criminal Purposes, New York – 29 Aug - 9 Sep 2022
- Participated in GFCE Annual General Meeting in Hague, Paris – 13 - 15 Sep 2022
- Guest Speaker, Central Security Clearing Systems (CSCS) Annual Event: The Future of Cyber Security, Abuja – 27 Oct 2022
- Facilitated the Computer Professionals Registration Council of Nigeria (CPrN) Mandatory Continuing Professionals Development (MCPD) - 3 Nov 2022
- Participated in the OIC-CERT 10th General Meeting & 14th Annual Conference 2022, Muscat – 7 - 9 Nov 2022
- NIMC WB Session "*Stakeholder engagement on Securely Enabling Access to Services through IDs*", Abuja – 14 - 15 Nov 2022
- Lecture on Cyber-threats and National Security in Nigeria: Imperatives for Resilience Cybersecurity Architecture at National Defence College, Abuja – 17 Nov 2022
- IGF 2022: Workshop on Cybersecurity for Development in 4IR, Addis Ababa, Ethiopia – 28 Nov - 2 Dec 2022
- Participated in George C. Marshall Centre Course for ECOWAS: "*The Framework of Responsible State Behaviour in Cyberspace – understanding the key elements, and implementation at the regional and national levels*" in Munich, Germany – 5 - 9 Dec 2022

3.3. Profile Summary

A Cyber Security, e-Library and ICT Policy Consultancy Firm.

Mission Statement: "To collaborate with, and empower, our clients by leveraging knowledge."

Motto: Collaboration. Empowerment.

Our collaborative culture means that we have linkages from around the world that provide the needed support required at short notice.

CS2 is peopled by a team of "Resourceful Managers" with strong bias towards the generation, sharing and utilisation of knowledge.

A flat core firm (CS2) that endeavours to empower its people to spin-off specialised firms, which they will operate as entrepreneurs.

4. PLANNED ACTIVITIES

- Increased involvement in the OIC CERT; Global Forum on Cyber Expertise (GFCE); African Union Cybersecurity Expert Group (AUCSEG); Global Commission on the Stability of Cyberspace (GCSC); Global ACE Certification; 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
- Implement in-house a cyber-forensics capacity development program
- Give services in support of the 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

  i. Implementation of the Nigeria National Cybersecurity Policy and Strategy

  ii. Implementation of National Data Protection Policy

  iii. Implementation of the Nigeria National Broadband Plan

  iv. Implementation of a Nigeria ICT Roadmap

  v. 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

  vi. Development of national frameworks and guidelines to protect Nigerian IT systems from deliberate attack from internal and/ or external forces

  vii. Implementation of a Nigeria "e"Trustmark to validate the e-Business activites, website security, apps, hardware, software, legality, and good "e"-Business behaviour

  viii. Establishment of a cadre of Information Security Professionals with direct reporting line to the Chief Executive of their assigned MDA as well as Office of Head of Information Security for the Nation at the National Information Technology Development Agency (NITDA)

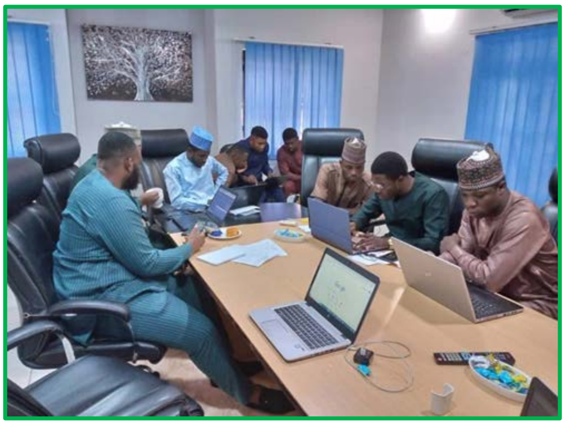
  ix. Establishment of local Cybersecurity Certification Authority with International credibility to increase number of cybersecurity professionals by leveraging on the *Global Accredited Cybersecurity Education (ACE) Scheme* and other partnerships

  x. Develop digital literacy and e-inclusion schemes for under-served communities, including women and girls

xi. Increase in compliance and adoption of IPv6 standards

xii. Strengthening of ICT departments in the Higher Education Institutions (HEIs)

xiii. Development of a blueprint of common services, policies, standards, procedures, and technical components that guide Ministries Departments and Agencies (MDAs) on IT investment



Cross section of the Participants during the 2022 2nd African Cyber Drill

Participants Group Photograph at 2nd African Cyber Drill 2022

Observers & Players at the African Cyber Drill

Players at the OIC-CERT Cyber Drill 2022

Observers at the OIC-CERT Cyber Drill 2022

Participants Group Photograph during the OIC-CERT Cyber Drill 2022

OMAN

Oman National CERT (OCERT)
Information Technology Authority

5. HIGHLIGHTS OF 2022

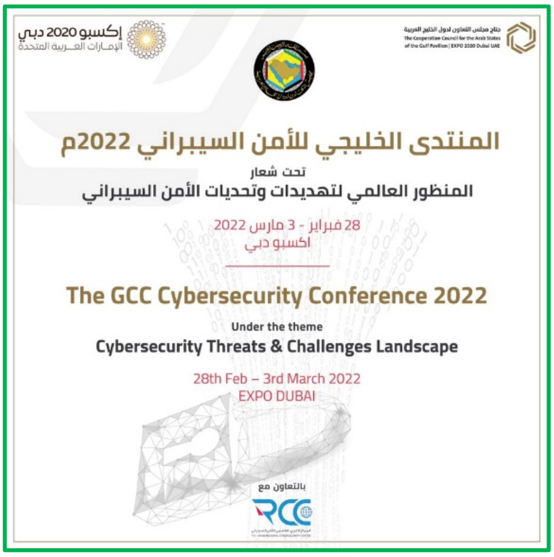
5.1. Summary of Major Activities

International Level

- Oman have been elected for the 5th times in a row as the Chair of the OIC-CERT
- Organized the cyber diplomacy initiative for Arab and Asia region in cooperation with the Center for Humanitarian Dialogue in Geneva
- Organized the 14th Annual Conference of the OIC-CERT in Muscat, Oman
- Participation in the organization and arbitration of the Global Cybersecurity Award of the OIC-CERT
- Organized the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions in Muscat, Oman
- Organized and chaired the 10th Annual General Meeting and the Board Meeting of the OIC-CERT in Muscat, Oman
- Chaired the Annual Meeting of the ITU- Arab Region Study Group 17 (SG17RG-ARB).
- Conducted the CERT assessment for Bahrain National CERT as a process for FIRST membership
- Organized the OIC-CERT Cyber Drill 2022
- Organized a cyber drill scenario for the Asia and Arab Region Conference in Kazakhstan
- Participated in a panel discussion on "*Cybersec Leadership - from Defence to Offence*" at the Exhibition World Bahrain

Regional Level

- Developed a cybersecurity Innovation framework for the Gulf Cooperation Council (**GCC**) CERT members


إكسبو 2020 دبي
الإمارات العربية المتحدة
جناح مجلس التعاون لدول الخليج العربية
The Cooperation Council for the Arab States of the Gulf Pavilion | EXPO 2020 Dubai UAE

المنتدى الخليجي للأمن السيبراني 2022م

تحت شعار

المنظور العالمي لتهديدات وتحديات الأمن السيبراني

28 فبراير - 3 مارس 2022
اكسبو دبي

The GCC Cybersecurity Conference 2022

Under the theme

Cybersecurity Threats & Challenges Landscape

28th Feb – 3rd March 2022
EXPO DUBAI

بالتعاون مع

RCC

- Developed an incident response plan for CTIGCC-CERT members
- Activating a secure link between the government network and the GCC network

- Organized the GCC Cybersecurity conference in EXPO Dubai 2022

- Organized the Regional Cybersecurity Week 2022 in Muscat, Oman
- Organized the 10th Regional Cyber Drill in Muscat, Oman
- Organized the 10th Regional Cybersecurity Summit in Muscat, Oman
- Organized the 3rd Women in Cybersecurity Middle East Conference in Muscat, Oman
- Organized and chaired the 10th Annual Arab Cybersecurity Cooperation Team (ACCT) meeting in Muscat, Oman

National Level

- Launched “*Hadatha*”, which is the Cybersecurity Industry Development Program
- Implemented the National Cybersecurity Index 2022
- The digital forensic lab is internationally recognized for the 7th time
- The National Digital Forensics lab dealt with 151 cases, including 843 digital evidence
- Organized the 8th National Cyber Drill in Muscat, Oman
- Participated in COMEX 2022 exhibition in Muscat, Oman

- Organized a workshop for freelancers in the field of cybersecurity
- Developed a guideline for the career path in cybersecurity
- Developed the cybersecurity Industry development framework
- Published 70 cybersecurity alerts and how to mitigate them
- Integrated 25 new PKI services with 18 government and private sectors
- 62 consultations service was delivered in the field of cybersecurity to government institutions

- Delivered 61 training for government institutions to manage protection devices
- Conducted on the job training for 14 graduate job seekers
- Conducted 4 penetration testing for government agencies

6. ABOUT THE ORGANIZATION/ AGENCY

6.1. Introduction

The Oman National Computer Emergency Readiness Team (**OCERT**) was established in 2010 to serve as a trusted focal point of contact on any ICT security incidents in the Sultanate of Oman. The focus is on cyber safety and security, capacity building and promoting cybersecurity awareness, and serve the public and private sector organizations, Critical National Infrastructure (CNI) as well as individuals

6.2. Resources

- *https://arcc.om/?GetLang=en*
- *https://arcc.om/pages/4/show/8*
- *https://cert.gov.om/default_ar.aspx*
- *https://rcssummit.com/*

Regional Cybersecurity Week 2022 Opening

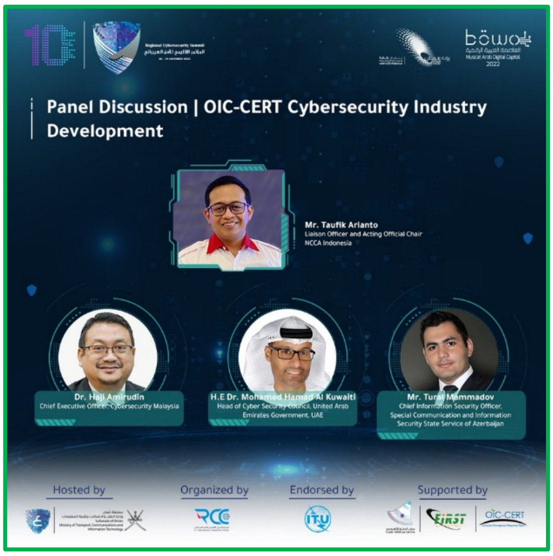
Regional Cybersecurity Week Activities

10th Regional & OIC-CERT Cyber Drill

OIC-CERT Board Meeting

OIC-CERT General Meeting

Re-election of OmanCERT as Chair of the OIC-CERT



Panel Discussion | OIC-CERT Cybersecurity Industry Development

Mr. Taufik Arianto
Liaison Officer and Acting Official Chair
NCCA Indonesia

Dr. Haji Amirudin
Chief Executive Officer, Cybersecurity Malaysia

H.E Dr. Mohamed Hamad Al Kuwaiti
Head of Cyber Security Council, United Arab Emirates Government, UAE

Mr. Tural Mammadov
Chief Information Security Officer, Special Communication and Information Security State Service of Azerbaijan

Hosted by Organized by Endorsed by Supported by

OIC-CERT Conference Activities

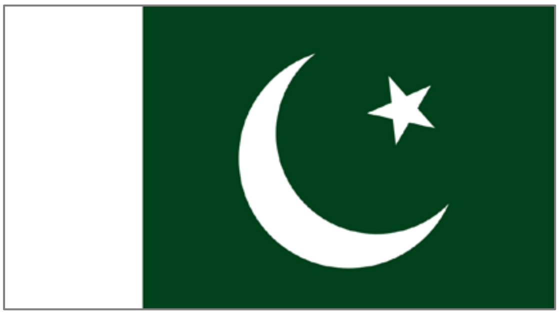
FIRST & ITU-ARCC Regional Symposium for Africa & Arab Region

10th Annual Arab Cybersecurity Cooperation Team (ACCT) Meeting

3rd Women in Cybersecurity Middle East Conference

The Asia & Arab Region Conference, Kazakhstan

World Exhibition Bahrain



PAKISTAN

Federal Investigation Agency CCW (NR3C)

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- Served as an active member of the OIC-CERT 5G WG
- Online participation in the OIC-CERT trainings
- Online participation in OIC-CERT organized or coordinated cyber drills
- Organized cybersecurity and cyber laws seminars in universities/ academic institutes across Pakistan
- Organized cybersecurity and cyber laws seminars in UET, KMU, KDC and IMSciences, Peshawar
- Organized cybersecurity and cyber laws seminars in FAST-NUCES, NUML, Islamabad Model College, SLS School, Froebel's International School, and convention centre Islamabad
- Organized cybersecurity and cyber laws seminars in PAF-KIET and Baharia University Karachi
- Organized cybersecurity and cyber laws seminars in the Rangers HQ, Lahore
- Organized cybersecurity and cyber laws seminars in BZU and National Highway & Motorway Police HQ, Multan

1.2. Achievements

- One female Forensic Expert of Federal Investigation Agency (**FIA**) CCW HQ Islamabad is pursuing PhD in Cybersecurity from Air University Islamabad
- One male Forensic Expert of FIA CCW HQ Islamabad is pursuing PhD in Cybersecurity from NUST Islamabad
- Muhammad Akram Mughal, Deputy Director Network Security FIA Cyber Crime Wing (NR3C) attained the credential of Computer Hacking Forensic Investigator (CHFI) after passing rigorous four hour exam conducted by EC-Council USA

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Establishment

- NR3C was established in 2007 as a PSDP funded project
- All officers and manpower of NR3C was regularized in 2012
- All officers inducted in Phase-II of NR3C are in the process of regularization (permanency)
- NR3C's inducted officers in Phase-III are serving as the employees of the Project. Process of

regularization has been initiated for said employees of NR3C

2.2. Resouces

- NR3C is a state-run wing of FIA. The resources required to meet the organizational objectives are provided by the state of Pakistan
- Resources allocated/ allotted by the state are financially sponsored through the Agency's budget or through PSDP funded projects
- NR3C is a state run organization and the state of Pakistan allocate resources to meet the organizational objectives
- NR3C promotes the interests of the state of Pakistan at the national and international level.
- NR3C is a full member of the OIC-CERT since the first seminar in 2009 in Kuala Lumpur, Malaysia. Therefore, objectives of NR3C are aligned with the objectives of OIC-CERT
- The manpower of NR3C comprises of four hundred and seventy-seven (477) well trained staff

2.3. Constituency

State of Pakistan public, national, and international domain

3. ACTIVITIES AND OPERATIONS

3.1. Events organized by the organization/ agency

FIA CCW organized seminars regarding

- cyber laws and cybersecurity for students and faculties in UET Peshawar
- securing smart phones and laptops in Khyber Medical College Peshawar
- cyber laws in Khyber College of dentistry
- cybersecurity, cyber laws and digital forensic in the Institute of Management Sciences Peshawar
- prevention of cyber crimes in the National University of Modern Languages (NUML) University Islamabad
- cybersecurity and cyber crimes in FAST-NUCES Islamabad
- the prevention of cyber crimes: laws in PAF-KIET Karachi
- the prevention of cyber crimes in Bahria University Karachi
- cyber laws in BZU Multan
- cyber laws at the National Highway and Motorway Police HQ, Multan
- cyber laws at the Rangers HQ, Lahore

British Council Peshawar and Umer Asghar Foundation jointly organized seminar in Serena Hotel Peshawar. Muhammad Akram Mughal, Deputy Director Network Security FIA CCW (NR3C) deliver a lecture on "Digital Safety and Security of Women and Children in KPK through Prevention of Electronic Crimes Act, 2016"

3.2. Events involvement

FIA CCW officer delivered a lecture as guest speaker on

- cybersecurity in IBA Karachi
- cybersecurity in GCWU Sialkot
- cyber laws in CLLB Peshawar
- cyber laws in CECOS University Peshawar
- cyber laws in Shaheed Benezir Bhutto Women University Peshawar
- cybersecurity in IMSciences Peshawar
- cyber laws in Frontier Law College Peshawar
- Cybersecurity Threat Intelligence in Metrix Tech Summit Hazara University, Mansehra
- Cyber Laws in NIM Peshawar
- Digital Safety of Women and Children in KPK through PECA, 2016 in Serena Hotel Peshawar. Event was organized by the British Council and Umer-Asghar Foundation
- cybersecurity and cyber laws in the Convention Centre of Islamabad

4. 2023 PLANNED ACTIVITIES

- To minimize cybercrimes in Pakistan through effective enforcement of Prevention of Electronic Crimes Act 2016 and coherent/ concerned clauses of Pakistan Penal Code as well as Pakistan Telecommunication Re-Organization Act, 1996
- Planning to open a Cyber Crime Report Centre (CCRC) in every district
- To strengthen the cyber patrol unit in FIA CCW
- To regularize contractual manpower of FIA CCW
- To minimize cyber crimes through effective and aggressive awareness campaign on cyber crimes and cybersecurity. To meet this end, seminars on cyber crime laws, digital forensics and cybersecurity will be organized in all major universities of Pakistan

Muhammad Akram Mughal of NR3C delivering a lecture on "Cyber Crimes: Risks and Countermeasures" at CECOS University Peshawar

Muhammad Akram with eminent scientists from the OIC member states during COMSTECH Conference on "Science Communication and Community Engagement" at COMSTEC Secretariate Islamabad, Pakistan

NR3C delivering a lecture on "Illustration of Technical Terms in National Cyber Crime Laws" at the Centre for Learning Law and Business (CLLB), Peshawar

FIA Cyber Crime Wing Peshawar seminar on "Cyber Security, Cyber Laws and Digital Forensic" in Khyber Medical College, Peshawar

FIA Cyber Crime Wing Peshawar organized seminar on "Cyber Security, Cyber Laws and Digital Forensic" in Khyber College of Dentistry, Peshawar

NR3C invited by Faculty of Law, Shaheed Benezir Bhutto Women University to deliver a lecture on "Illustration of Technical Terms in National Cyber Crime Laws"

NR3C was hnoured by Dr. Syed Irfan Nabi, HOD, IBA CICT after his lecture at IBA on cybersecurity

NR3C invited by HOD Computer Science Department, Government College Women University Sialkot to deliver a lecture on "Cybersecurity for Students and Faculty" and conduct workshop on "How to Secure Laptopts and Smart Phones"

NR3C invited by the President Bar Council Pasrur to deliver a lecture on "Illustration of Technical Terms in National Cyber Crime Laws"

NR3C serving as penalist and speaker during Metrix Tech Summit at Hazara University, Mansehra, KPK on "Cyber Threat Intelligence"

NR3C conducting training session on "Illustration of Technical Terms in National Cyber Crime Laws" at Shakas Police Training College Peshawar

FIA CCW (NR3C) Lahore: Cyber Crime Awareness Seminar at Rangers HQs. Lahore

FIA CCW (NR3C) Karachi organized a seminar on Cybersecurity at PAF-KIET Karachi

FIA CCW (NR3C) Islamabad organized seminar on cyber crimes awareness at NUML

FIA CCW (NR3C) Karachi organized Cyber Crimes Awareness at Baharia University Karachi

FIA CCW (NR3C) organized the National Cyber Crime Laws for National Highway and Motorway Police Multan

FIA CCW (NR3C) Islamabad conducted awareness session on Cyber Crimes and Cyber Security at Convention Centre Islamabad during Kamyab Khawateen conference attended by two Federal Ministers and around 4000 women audience

Pakistan Information Security Association (PISA-CERT)

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- APCERT Cyber Drill 2022 – 25 Aug 2022

APCERT Drill 2022

- CERT Training: Incident Response & Medical Device Reporting (**MDR**) – 22 Aug 2022
- Digital Forensics Workshop – 23 Aug 2022
- Training on "*Role of CERT in 21st Century*", National Electric Power Regulatory Authority (**NEPRA**) – 4 Nov 2022
- Conference "*Sustainable Cyber Secure Pakistan Vision 2030*" – 24 Aug 2022
- Seminar "*Preparing Workforce For 21st Century*", International Islamic University Islamabad – 22 Nov 2022

Preparing Workforce for 21st Century

- The 10th Arab Regional & OIC-CERT Cyber Drill – 06-07 Nov 2022
- Panel Discussion "*Role of CERT in 21st Century Cyber Security*" – 30 Nov 2022
- 2nd Africa international OIC Cyber Drill 2022 – 9 Sep 2022

1.2. Achievements

In 2022 PISA has completed the following target

- Participated in the International Cyber Drills
- Conducted seminars/ workshops on cybersecurity
- Participated in the National and International Competition (CTF/ CyberLympics)

Several students and professionals (universities, law enforcement) have been trained in cybersecurity and information security by PISA-CERT

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

The Pakistan Information Security Association (**PISA**) is a not-for-profit organization working in the information security domain at different levels nationally and internationally. PISA is working with all the relevant stakeholders from the public and private organizations for educational interaction opportunities that enhance the knowledge, skill, and professional growth of the members

The primary goal of PISA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources

PISA facilitates interaction and education to create a more successful environment for global information systems security and professionals' involvement

2.2. Establishment

PISA was establishment in 2005

2.3. Resources

- Information Security Experts
- Cybersecurity Experts
- Digital Forensic Experts
- Incident Response Experts
- Penetration Testing Experts
- SOC Specialists
- Information Security Management
- Network Security Specialist

2.4. Constituency

Pakistan

3. ACTIVITIES AND OPERATIONS

3.1. Events organized by the organization/ agency

- CERT Training: Incident Response & MDR – 22 Aug 2022
- Digital Forensics Workshop – 23 Aug 2022

Digital Forensics Workshop

- Training On "*Role of CERT in 21st Century*", NEPRA – 4 Nov 2022
- Conference "*Sustainable Cyber Secure Pakistan Vision 2030*" – 24 Aug 2022
- Seminar "*Preparing Workforce For 21st Century*", International Islamic University Islamabad – 22 Nov 2022
- Panel Discussion "*Role of CERT in 21st Century Cyber Security*" – *30 Nov 2022*

3.2. Events involvement

- APCERT Cyber Drill 2022 – 25 Aug 2022
- The 10th Arab Regional & OIC-CERT Cyber Drill – 06-07 Nov 2022
- 2nd Africa International OIC Cyber Drill 2022 – 9 Sep 2022

3.3. Achievement

In 2022 PISA have achieved all targets set in 2021. Participated in the international cyber drills and successfully organized seminars and workshops. Provide services to law enforcement, public and private sectors in the following

- Guidelines to minimize threats of Ransomware
- Identifying and responding to server-level threats
- Security assessments of different infrastructures
- Responding to the cyber incidents

4. 2023 PLANNED ACTIVITIES

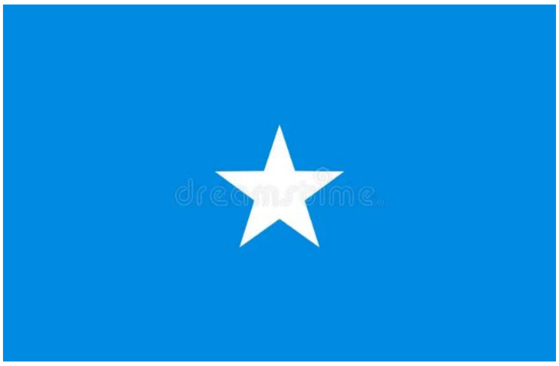
- Planned to organize international cyber drill on 14 Aug 2023
- Planned to organize Cyber Secure Pakistan International event
- Planned to participate in the International Cyber Security Drills, CTF competition, CyberLympics
- Planned to organize cybersecurity/ information security seminars and workshops for universities, government, and private sectors

Training On “Role of CERT in 21st Century”, NEPRA – November 04,2022

Conference “Sustainable Cyber Secure Pakistan Vision 2030”

CERT Training: Incident Response & MDR

Panel Discussion “Role of CERT in 21st Century Cyber Security”



SOMALIA

Somalia Computer Emergency Response Team/ Coordination Centre (SomCERT/ CC)

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- Serve as a trusted point of contact at the national level
- Provide cybersecurity incident handling
- Develop policies, procedures, and guidelines
- Provide advice to the stakeholders
- Manage and release cybersecurity alters
- Provide cybersecurity training and education
- Raise Cybersecurity Awareness Campaign
- Collaborate with the local and international CERTs

1.2. Achievements

- The President of Somalia signed the National Data Protection Law and published it in the Official Gazette of the Federal Republic of Somalia.
- Developing the National Cybersecurity Strategy and Policy
- Developing the Cyber Crime Act
- Enhancing the National CERT

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

The Somalia Computer Emergency Response Team/Coordination Center (**SomCERT/CC**) is the first national CERT in Somalia. SomCERT/CC provides cybersecurity incident handling, promotes cybersecurity awareness, as well as coordinating cybersecurity issues. SomCERT/CC collaborates with government agencies, organizations, telecom operators, National Critical Infrastructure Providers, Academia, ISPs, and other relevant entities to handle cybersecurity incidents in Somalia and various cybersecurity initiatives worldwide. SomCERT provides timely warning, support, and advisories to its constituents in preventing and handling cybersecurity incidents

2.2. Establishment

SomCERT/CC was established in 2019, by the National Communications Authority (NCA) of Somalia, as a section under the Cybersecurity Department to secure Somalia's cyber space and provide an official point of contact to handle cybersecurity incidents for the Internet community

2.3. Resources

- Incident Handling and Response Team
- Cyber security training and awareness team
- Information Sharing team
- International Coordination team
- Cybersecurity Awareness Campaign Team

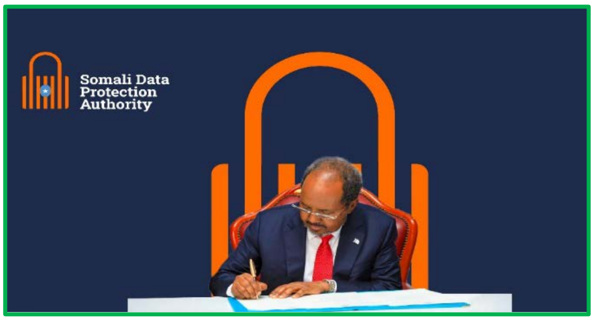
2.4. Constituency

- Ministries and government agencies
- Law Enforcement agencies
- Regulatory bodies
- National defence
- Banks and finance
- ICT, ISP, and telecommunication providers
- Academia
- National Critical Infrastructure Providers

3. ACTIVITIES AND OPERATIONS

3.1. Events organized by the organization/ agency

- SOMCERT staff attended the Introduction to *Ethical Hacking Traning* in Nairobi – Kenya
- SOMCERT participated in *Girls in ICT Week 2022*
- SOMCERT participated in the National Data Protection Law assessment



3.2. Events involvement

- Participated in the 10th Arab Regional Cyber Drill 2022 organized by ITU-ARCC
- Participated in "*Cloud Computing Security: Challenges & Opportunities for Public Sectors*" hosted by CyberSecurity Malaysia Awards, Conference & Exhibition (CSM-ACE)
- Attended ITU Global CyberDrill 2022

- Participated in FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions
- Participated in the *"Global Digital Security and Forensic 2022 - Future & Trends government Sector: Emerging Threats in Social Media: Technology and Policy"*

4. 2023 PLANNED ACTIVITIES

- Building the Malware Analysis Laboratory
- Improving the current National CERT and enhancing the existing capabilities of SOMCERT
- Developing the National Cybersecurity Strategy and Policy
- Developing the Cybersecurity and Cybercrime Legislation
- Developing the National Guidelines for the Protection of CII
- ISO 27000-series or similar Cybersecurity certification for SomCERT
- Assessment for establishing a cyber forensics laboratory for law enforcement with estimates and technical specifications
- Establishing a School of Cybersecurity

TUNISIA

National Agency for Computer Security (Tunisian Computer Emergency Response Team – tunCERT)

5. HIGHLIGHTS OF 2022

5.1. Summary of Major Activities

- organization of several awareness sessions
- cyber incident response
- provide immersion missions for the benefit of African CERTs
- cyber drill organizations for the benefit of African CERTs

5.2. Achievements

- organization of several awareness sessions
- cyber incident response
- provide immersion missions for the benefit of African CERTs
- cyber drill organizations for the benefit of African CERTs

6. ABOUT THE ORGANIZATION/ AGENCY

6.1. Introduction

ANSI, as the national coordinator, works to develop a climate of trust in information technology among the users, the state, and investors, apart from protecting citizens and public and private assets against any cyber threat

6.2. Establishment

The agency carries out a general control of the computer systems and the networks belonging to various public and private organizations, it is tasked with the following missions

- To ensure the implementation of the national guidelines and the general strategy in security systems of computer systems and networks
- To follow up on the execution of plans and programs related to computer security in the public sector, except for the particular applications of defense and national security, and to ensure the coordination between the actors in this field
- To ensure technological watch in the field of computer security
- To establish standards specific to computer security and to elaborate technical guides on the subject and to proceed with their publication
- To encourage the development of national solutions in the field of computer security and to promote them according to the priorities and

the programs which will be determined by the agency

- To participate in the consolidation of training and retraining in the field of computer security
- To ensure the execution of regulations related to the obligation of the periodic audit on the security of computer systems and networks

6.3. Resources

- The National Information Security Agency Departments:
- Executive management
- The unit of Prospection and Technological R&D
- The Management Control and Quality Management Unit
- Resources Management
- Computer Systems Security Technologies Unit
- Information Systems Security Audit
- IT Emergency Response and Support Department

6.4. Constituency

Tunisia computer and Internet users

7. ACTIVITIES AND OPERATION

7.1. Events organized by the organization/ agency

Cybersecurity Innovation Summit 2022 Tunisia – *16 Sep 2022*
https://msevents.ae/cybersecurity-innovation-series-tunisia-home-page/

7.2. Events involvement

Security & Cloud Expo (1st edition) – *25-26 May 2022*
https://www.facebook.com/photo/?fbid=418540353608034&set=a.419731530155583

7.3. Achievement

- Cybersecurity Innovation Summit 2022 Tunisia – *16 Sep 2022* https://msevents.ae/cybersecurity-innovation-series-tunisia-home-page/
- Security & Cloud Expo (1st edition) - *25-26 May 2022* *https://www.facebook.com/photo/?fbid=418540353608034&set=a.419731530155583*

8. 2023 PLANNED ACTIVITIES

- Organize awareness sessions
- Organization of events
- Organization of cyber drills
- Organization of immersion missions to tunCERT

TURKEYE

Turkcell CDC

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

In 2022, Turkcell CDC continued to offer new cybersecurity services for the corporate and individual customers

Threat Intelligence Service (Bozok)

Turkcell CDC launched a threat intelligence platform called Bozok, which provides an up-to-date IOC information, threat actor reports, mobile app tracking, ransomware tracking data leak detection, brand protection and vulnerability detection services to the corporate customers

BOZOK TI infrastructure is powered by nearly 100 intelligence sources. CDC EYE, dark web and threat intelligence forums, Pastebin, Github, Twitter, Virus Total etc. Detecting data leaks with automation and instant reporting, BOZOK enables its customers to take early action. Includes threat actor reports specific to advanced APT groups. It detects newly opened domains and warns customers against phishing attacks. It offers a "*Malware Analysis*" interface to examine files that customers suspect. Provides information about existing vulnerabilities with vulnerability centre. The number of customers increased by 114% in 2022, thanks to the works carried out in this context

Turkcell Security Operation Centre Service

The organization offers a 7x24 SOC services to the customers with the mission of creating added value for national cybersecurity and the vision of increasing cyber resilience by providing community cybersecurity. We produce innovative ideas and develop quality products and services, and in this context, we try to keep customer satisfaction at the highest level. Apart from the 24/7 monitoring service, we provide various trainings by expert cybersecurity engineers in order to create cybersecurity awareness and feed the customers with monthly reports such as critical vulnerability notifications and security recommendations. As a result of these efforts, the number of customers increased by 67% in 2022

Digital Security Services

Turkcell Digital Security Service is a solution designed specifically for Turkcell's mobile Internet users. As phishing & fraud attacks continue to become more sophisticated, persistent, and adapt to mobile security defences, demand for phishing & fraud defence solutions is at an all-time high. Turkcell Digital Security Service ensures the users are making traffic only with safe endpoints. This service alerts users of any suspicious connection attempts or links with the help of machine learning and artificial intelligence algorithms.

Also, the service informs the customers, if they are using e-mail and social media accounts that have leaked passwords

Turkcell Security Orchestration, Automation and Response (SOAR) Service

As a result of digital transformation, both the number of security vulnerabilities and threats to information technology systems are in an increasing trend. Turkcell CDC Security Engineers are experts and have the ability to respond to cyber incidents accurately and quickly using industry standard methodologies. In this context, Turkcell CDC launched Turkcell SOAR in 2021 for both Turkcell internal and SOC service customers to allow faster and safer action by the engineers. As a result of various studies and developments carried out, the number of customers increased by 100% in 2022

Mitre Att&CK Framework Compatibility and Purple Team

Turkcell examine and test the tactics, techniques and procedures of advanced attack groups as part of the efforts to comply with the Mitre Att&CK framework, which is accepted globally. Considering the motivations, the organization developed rules to detect any anomalies in the systems. With this study, 190 new rules were written in 2022 and the compliance rate was increased to 92%. In addition, the Purple Team was formed to improve Turkcell's general security, optimize efficiency and effectiveness, and try to maximize security. By imitating the attacks made by advanced attack groups and current attack vectors, information and insights about corporate security are reported and shared with all security team managers monthly.

Digital Forensics and Incident Response Service

Turkcell DFIR Service covers the identification, examination, and determination of action plans of all kinds of violations that may occur against cyber attacks, assets that are in the position of open targets and that threaten information and data security. Case studies have been conducted with up-to-date technologies by Turkcell engineers, who have high level of knowledge, in more than 1000 cyber-attacked businesses. After these investigations, the main items such as why and how the incident occurred, customer information assets, the effects and risks it created on business processes, systems affected directly or indirectly, determination of the root cause, what are the measures to be taken to prevent the incident from recurring were determined and reported for action

Cyber Security Trainings

Various trainings are provided by Turkcell cybersecurity engineers, who are experts in their fields, in order to increase the information security awareness of corporate customers at Turkcell CDC. These trainings are as follows

- Cyber Security 101 and Phishing Training
- Threat Intelligence Training
- SIEM Management Training
- Windows Forensic Tutorial
- Malware Analysis Training

CDC Sense Honeypot

The CDC Sense project, which enables Turkcell to look at events from a larger perspective by tracking cyber attacks around the world in more detail, and thus allowing the organization to reach first-hand attack forms such as command and control centre and malware used in attacks, has been completed by analysing attacker profiles. With this project, in which decoy systems located in 11 countries are developed, enriching threat intelligence infrastructure and contributing to the increase of intelligence quality, raw data that are not shared or not shared in different intelligence networks are analysed gradually and added to the BOZOK Threat Intelligence infrastructure.

Signalling Security

Within the scope of the signalling security project, Turkcell created an alarm mechanism on SS7, Diameter, GTP and 5G security for anomaly detection with the analysis obtained by collecting the electronic signalling traffic. In addition to providing a high level of security and multi-layer protection in subscriber bases, Turkcell take preventive actions without being exposed to attacks by revealing known/ potential new security risks, and we develop use cases here to minimize the risk in the face of attacks

1.2. Achievements

Turkcell CDC CTF teams participated in many CTF events in 2022 and ranked high. Some of these CTFs are African Cyber Drill, EGCERT 2022, APCERT 2022, and STM CTF 2022.

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

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 centre 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, Continuous Vulnerability Services, Attack Surface Management Services, MDR/ XDR Services, SIEM Consultancy are also provided

2.2. Establishment

Turkcell CDC is established in December 2015

3. ACTIVITIES AND OPERATION

3.1. Events organized by the organization/ agency

Turkcell participated in the activities within the scope of Cyber Security Week, which was held between Nov 30 and Dec 2 2022 under the coordination of the Turkish Cyber Security Cluster under the auspices of the Presidency of Defense Industries and the Presidency's Digital Transformation Office. The organization gave information about the services and trainings to the visitors and presentations on Threat Intelligence platform BOZOK, SOC Service, Digital Security Service

Cyber Security Week 2022

3.2. Events involvement

Turkcell CDC members made presentations and gave trainings on various cybersecurity issues at Technology Talks, Cyber Security Week, MicroFocus Event, Information Security Association, and IDC conferences. Turkcell CDC attended the Turkey Cyber Security Cluster Week and made presentations on various topics such as BOZOK Threat Intelligence, Digital Security Service. Turkcell CDC also attended the CDC's Microfocus Universal Conference in 2022, where Turkcell CDC shared experiences with state-of-the-art distributed ESM infrastructure for customers purchasing SOC Service

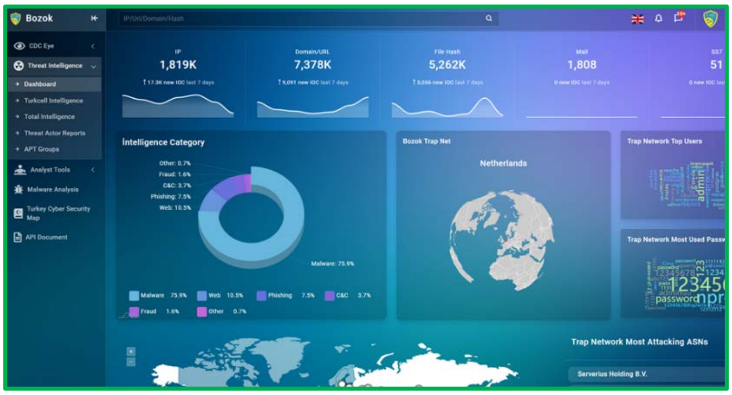
3.3. Achievement

Turkcell CDC CTF teams participated in many CTF events in 2022 and ranked high. Some of these CTFs are: African Cyber Drill, EGCERT 2022, APCERT 2022, and STM CTF 2022

4. 2023 PLANNED ACTIVITIES

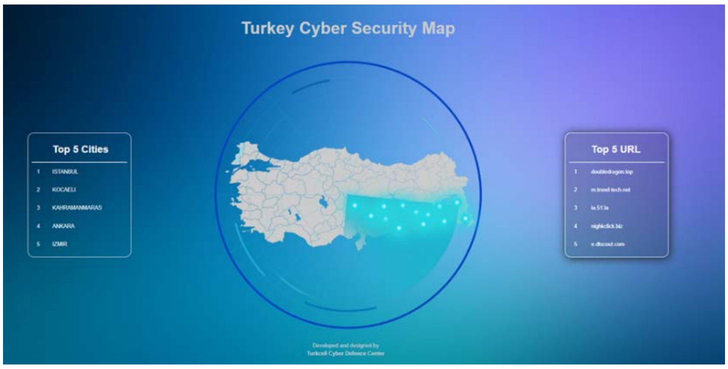
- Reaching more foreign customers by improving overseas customer work
- Providing MDR Service to the customers
- Use case development for product dissemination and detection of any suspicious activity within the scope of SCADA security project

E-Safe Cyber Security Conference 2022



Turkcell CDC Bozok Threat Intelligence Service

Cyber Security Week 2022- BOZOK Threat Intelligence Platform Presentation


Turkey Cyber Security Map
Top 5 Cities
1 ISTANBUL
2 KOCAELI
3 KAHRAMANMARAS
4 ANKARA
5 IZMIR
Top 5 URL
Developed and designed by
Turkcell Cyber Defence Center

Turkey Cyber Security Risk Map

Turkcell Cyber Defence Center

UNITED ARAB EMIRATES

UAE Computer Emergency Response Team (aeCERT)

5. HIGHLIGHTS OF 2022

5.1. Summary of Major Activities

- Cyber Pulse Initiative

Cyber Drills

The UAE Cybersecurity Council (**CSC**) conducted a total of 12 cyber drills

The cyber drills were attended by over 500 individuals

The drills covered 8 distinct topics related to cybersecurity

The drills were targeted at 70 federal and government entities

Future leaders

The UAE Cybersecurity Council conducted 20 cyber awareness sessions targeted at C-suite executives, directors, and managers

The sessions were attended by 105 individuals, including high-level leaders from government and international entities

The sessions covered 8 diverse topics related to cybersecurity

The awareness sessions were specifically targeted at 70 federal and government entities to help them build their cybersecurity awareness and capabilities

Cyber Pulse for the Society

The UAE Cybersecurity Council conducted 52 cyber awareness sessions

These sessions were attended by 92,000 people from various segments of the society, including families, senior citizens, and students.

The sessions covered 32 diverse topics related to cybersecurity, ranging from basic cyber hygiene to more advanced topics such as social engineering and identity theft

The council targeted 13 different societal entities, including universities, schools, and general women's union

Developed and published cybersecurity awareness digital packages containing infographics, social media posts, and other relevant materials

Computer Emergency Response Services

238 cyber incidents have been dealt with

1196 sites were monitored against defacement

Cyber Security Awareness Services

57 awareness sessions provided

4457 people attended awareness sessions

Security Quality Services

30 vulnerability reports prepared
72 vulnerability assessment testing
49 vulnerability assessment testing

Cyber Security Monitoring

15 endpoints protection provided
25 SIEM solutions provided for entities

- Collaborations with Global Partners

  - The CSC entered into MoUs with the following international partners to enhance cybersecurity strategies

    i. CPX
    ii. Oracle
    iii. Microsoft
    iv. Hewlett Packard Enterprise
    v. Kela
    vi. IBM
    vii. SAP
    viii. AWS
    ix. IDC
    x. Huawei
    xi. KPMG
    xii. Madinat
    xiii. CyberArrow
    xiv. Immersive Labs

  - The CSC has joined the Gartner Research Board, underscoring the country’s growing international stature and pivotal role in the area of cybersecurity

  - The CSC signed a cooperation agreement with Saudi Arabia's National Authority for Cybersecurity

  - The CSC provided their feedback on an ITU resolution regarding questions and considerations related to online cyber crime and child online protection

  - The CSC was featured at the IDC Middle CIO Summit sharing exclusive insights on the UAE cybersecurity ecosystem

  - The CSC represents the UAE at the European Cybersecurity Challenge 2022 in Vienna, Austria. Several security-related challenges from domains such as web security, mobile security, crypto puzzles, reverse engineering, and forensics took place to support young cyber talents and increase awareness about cybersecurity

- The CSC with other UAE entities such as TDRA, participated in a hybrid meeting at EXPO 2020. The main objective was to highlight cybersecurity in the transportation sector

- The CSC represented the UAE at the ITU Arab Inter-regional Cyber Drill organized by the ITU in Kazakhstan in Sep 2022
- During the World Government Summit 2022, an initiative was introduced to extend the UAE's digital transformation expertise to African nations. The initiative involves conducting workshops with the involvement of 18 countries with the aim of facilitating knowledge transfer to these friendly African countries
- The CSC signed a MoU with Amazon Web Services (AWS) to enable faster adoption of AWS cloud services by the UAE's public sector and regulated industries, including healthcare and financial services, leveraging on the AWS's global cloud infrastructure
- The CSC signed a MoU with Spain's Minister of Foreign Affairs, European Union and Cooperation
- The CSC and Deloitte signed a MoU to engage in collaborative activities supporting the cybersecurity agenda in UAE. The MoU will enable CSC and Deloitte to collaborate and leverage Deloitte's expertise and experience in UAE cybersecurity while drawing on internationally recognized good-industry practices to support the UAE Cybersecurity Agenda.
- A MoU was signed between CSC and Cisco to strengthen cybersecurity strategies and initiatives in the country. The collaboration between the two entities is focused on creating a robust cybersecurity framework, developing cybersecurity skills, and enhancing the capabilities of the cybersecurity system. The goal is to address the growing demand for digital technologies in institutions across the public and private sectors and ensure that they are implemented securely. By partnering with Cisco, the CSC aims to further enhance the country's cybersecurity infrastructure and build a resilient cybersecurity ecosystem that can respond to emerging threats in a timely and effective manner
- The CSC participated in the ADDA CTF competition held in Scotland, bringing together cyber professionals and enthusiasts from around the world to test their skills in solving cybersecurity challenges. The competition was a platform for the exchange of knowledge and expertise in the field of cybersecurity, as well as an opportunity to enhance the UAE's

reputation as a leader in the field of cybersecurity

- Political Collaborations

- The CSC has established political collaborations with various organizations, to enhance the country's cybersecurity capabilities and promote international cooperation
  - i. ITU
  - ii. Open-Ended Working Group (OEWG)
  - iii. Centre for Humanitarian Dialogue (HD)
  - iv. International Counter Ransomware Initiative (**CRI**)

- The CSC joined 37 international organizations from the public and private sectors to discuss ways of combatting the spread and impact of ransomware at the CRI 2022. The CRI was held in Washington, DC on 31 Oct and 1 Nov under the auspices of the US White House, attended by the US Vice President Kamala Harris

- The CSC participated in the GCC Cybersecurity Ministerial Committee meeting in Riyadh, Saudi Arabia

- The CSC participated in the Global Cybersecurity Forum concluded in Riyadh

- The CSC participated in four scenarios developed by the ARCC and the ITU on national centres for cybersecurity and emergency response in Arab and OIC countries

- The CSC participated in the CSIS - Tunisia Chapter conference, which was organized by the Centre for Strategic and International Studies. The conference aimed to discuss and showcase the latest advancements in the field of cybersecurity and to explore the opportunities and challenges that arise from them. It brought together experts, professionals, and decision-makers from various sectors to exchange knowledge, ideas, and best practices related to cybersecurity

- The CSC participated in the QNA Security Conclave & Awards event, which aimed to recognize and honour individuals and organizations for their outstanding contributions to the field of cybersecurity

- The CSC's participation in the Product-to-Consumer (P2C) initiative to establish strong links with the target countries and communities i.e the Least Developed Countries (LDCs), Landlocked Developing Countries (LLDCs) and Small Island Developing States (SIDS) and help strengthen UAE's position within international multi-stakeholder alliances and support the overall eminence in the international cybersecurity landscape

- The CSC participated in the ITU World Telecommunication Development Conference (WTDC) in

Rwanda to discuss future collaboration and mechanisms to enhancing cooperation on cybersecurity, including countering and combatting spam

- Collaborations with National Entities

o The CSC has signed MoUs with various local and government entities to improve cybersecurity measures in the UAE

i. Federal Authority For Government Human Resources
ii. Department of Energy - Abu Dhabi
iii. EDGE
iv. Cyber Gate
v. Injazat
vi. Khalifa University

o The CSC has joined the Ministry of Industry and Advanced Technology's National In-Country Value Program

o The CSC and the Department of Health jointly conducted cyber drills aimed at enhancing the sector's readiness to deal with cyber threats. The drills involved the simulation of various cyber-attack scenarios to evaluate the department's response mechanisms and identify areas that require improvement. Through these drills, the CSC and Abu Dhabi Department of Health aimed to raise awareness about the importance of cybersecurity in the healthcare sector and to equip healthcare professionals with the necessary skills and knowledge to effectively manage and mitigate cyber risks. The collaboration between the two entities highlights the UAE's commitment to strengthening its cybersecurity posture and ensuring the protection of critical sectors from cyber threats

o The CSC signed a MoU with the Emirates Nuclear Energy Corporation (ENEC) to support the development and review of national-level strategies, policies, and standards for the cybersecurity of the UAE energy sector

o In collaboration with the educational institutions and national universities, the CSC conducted cyber drills to strengthen the response capabilities of the education sector to cyber threats. The exercises involved multiple presentations to simulate various cyber-attack scenarios, aiming to identify monitoring and response mechanisms and enhance the readiness of educational institutions to deal with such incidents proactively and professionally. The cyber drills were part of a series of simulation exercises aimed at enhancing the overall cybersecurity posture of the country

5.2. Achievements

Guinness World Record

- The CSC achieved a Guinness World Record for hosting the most users in a CTF video hangout
- The CSC achieved a Guinness World Record for hosting the largest bug bounty competition at the GISEC 2022

Global and International Achievements

- As a result of the CSC's participation in the GCC Cybersecurity Ministerial Committee meeting in Riyadh, the following achievements were made
  - i. Unified Gulf Cloud established to strengthen cybersecurity in the region
  - ii. Gulf Testing and Auditing Laboratory being developed for enhanced cybersecurity
  - iii. Gulf Security Operations Centre adopted to bolster regional cyber defenses
  - iv. New Anti-Ransomware Mechanisms formed in the Gulf region to combat cyber threats

GUINNESS WORLD RECORDS
CERTIFICATE
The largest cyber drill competition was achieved by Cyber Security Council (UAE) in Dubai, United Arab Emirates on 15 January 2022
OFFICIALLY

- The CSC elected as the Deputy Chair of the OIC-CERT to respond to cyber emergencies
- The "Cyber Plus Innovation" centre, which focuses on cybersecurity and cyberspace, was launched at Abu Dhabi Polytechnic, a subsidiary of the Abu Dhabi Technical Institute. The centre was established in partnership with the CSC and Huawei International and is dedicated to fostering innovation in the field of cybersecurity. With this collaboration, the centre aims to leverage the expertise and resources of partners to develop cutting-edge cybersecurity solutions and technologies. Through advanced training programs, the centre also

aims to equip individuals and organizations with the skills and knowledge needed to tackle the ever-evolving threats in the cyber landscape

6. ABOUT THE ORGANIZATION/ AGENCY

6.1. Introduction

https://csc.gov.ae/

The UAE Cabinet granted approval in Nov 2020 for the establishment of the CSC, a federal entity with the mandate to create and implement a comprehensive cybersecurity strategy aimed at strengthening the nation's cyber infrastructure. The council's primary objective is to promote a secure and safe cyber environment in the UAE by enhancing cybersecurity practices and protecting CII from cyber threats. Its formation is a critical component of the UAE's broader national cybersecurity strategy, which seeks to position the country as a leader in cybersecurity and facilitate digital transformation

aeCERT international participation

- Membership in OIC – CERT
- Membership in GCC- CERT
- Membership in ARCC
- Membership in ITU Child Protection Working Group
- Member of FIRST

6.2. Establishment

aeCERT was established by the Decree 5/89 of 2008 issued by the Ministerial Council for Services. The CSC established by the UAE Cabinet in Nov 2020

6.3. Resources

Services

- Policy and Strategy Development
  - o Developing national cybersecurity policies and strategies
  - o Conducting cybersecurity risk assessments and providing recommendations
  - o Providing guidance on regulatory compliance and best practices

- Capacity Building and Training
  - o Delivering cybersecurity training and awareness programs for different target groups, including government entities, private sector organizations, and the general public
  - o Offering professional development courses and certifications to enhance the cybersecurity skills of professionals in the field

- Incident Response and Management
  - o Conducting investigations and analysis of cybersecurity incidents to identify and mitigate potential threats
  - o Offering advisory services and technical support to organizations experiencing cybersecurity incidents

- Research and Development
  - o Conducting cybersecurity research and analysis to inform policy and strategy development

- Collaborating with local and international partners to promote innovation and knowledge exchange in the field of cybersecurity

- International Cooperation:
  - Establishing partnerships and collaborations with local and international organizations to enhance the UAE's cybersecurity capabilities and promote global cybersecurity standards and best practices

- Security Quality
  - TrustAE
  - Vulnerability Assessment
  - Mobile Application Scan
  - Source Code Review
  - Phishing Assessment
  - Vulnerability Detection Report

- Security Monitoring
  - Endpoint protection providing security alerts to notify constituents of relevant cyber threats, as well as recommendation/ mitigation steps to harden their environment against cyber threats
  - SIEM Solution providing entities with the LogRhythm SIEM platform for managing and storing logs, alerts, and analytics

- Security Compliance
  - UAE IA Standard Auditing
  - Security Compliance Consultation

Training and Education

The CSC provides a variety of training and education programs to government agencies, private organizations, and the general public in order to improve cyber security awareness and understanding of cyber threats. Some examples of the types of training and education provided by the council include

- *Cyber security awareness training* - The council provides training and education to government agencies, private organizations, and the general public on cyber security best practices and how to protect against cyber threats

- *Technical training* - The council provides technical training to government agencies and private organizations on how to use cyber security tools and technologies to protect their networks and systems from cyber threats

- *Cyber incident response training* - The council provides training to government agencies and private organizations on how to respond to cyber incidents, including incident management, incident response, and incident recovery

- *Cybersecurity regulations and compliance training* - The council provides guidance and training to organizations on how to comply with cyber security regulations and standards

- *Cybercrime investigations and forensic training* - The council provides training to government agencies and private organizations on how to investigate and prosecute cybercrime

- *Cybersecurity awareness campaigns* - The council runs campaigns to educate the public about cyber security and the steps they can take to protect themselves from cyber threats

- *Cybersecurity education for students* - The council provides cybersecurity education to students and young people to raise awareness of cyber security and to encourage them to pursue cyber security-related careers

6.4. Constituency

- Federal government entities
- Local government entities
- Private sector organizations
- CII (e.g., energy, transportation, healthcare, etc.)
- Academic and research institutions
- International organizations and partners

7. ACTIVITIES AND OPERATIONS

7.1. Events organized by the organization/ agency

- The CSC has organized a number of international events aimed at enhancing the country's cybersecurity posture on a global scale
  - Intersec
  - IDC CIO
  - GISEC
  - 5G Mena
  - CyberTech Global UAE
  - Digital Transformation
  - GITEX
  - TECHSPO
  - Future BlockChain
  - HITB

- At GISEC 2022, the CSC launched the Bug Bounty challenge, which featured the largest cyber-battle ground. The Bug Bounty challenge brought together ethical hackers from various parts of the world to identify and fix security vulnerabilities in numerous devices, including electric cars, smartphones, and drones. The competition aimed to promote cybersecurity awareness, encourage the discovery of potential security flaws, and reward ethical hackers for their efforts. The Bug Bounty challenge was a massive success, with an impressive participation of over 600 ethical hackers from different parts of the world. The achievement of the Guinness World Record is a testament to the UAE Cybersecurity Council's commitment to promoting cybersecurity and building a resilient cybersecurity ecosystem in the country. It also highlights the progress made by the UAE in the field of cybersecurity and its ability to attract top cybersecurity talents from across the world

- The CSC achieved a Guinness World Record for hosting the most users in a CTF video hangout. The event was held on 8 Apr 2022, in Dubai, UAE, and had an impressive participation of 674 individuals. The Cyber-CTF challenge was part of the event, and participants competed to capture a cyber flag in a race against time. The challenge aimed to promote cybersecurity awareness and improve the skills of cybersecurity professionals. At the end of the competition, two participants managed to capture the flag. The achievement of the Guinness World Record demonstrates the CSC's commitment in promoting cybersecurity and the significant progress made in the country's cybersecurity landscape

- The CSC organized an unprecedented international drill at World Expo Dubai, which saw the participation of aviation and cyber authorities from various countries i.e. the US, Germany, Greece, Morocco, and Bahrain

- The CSC organized a cyber drill on the Italy Pavilion's stage at Expo 2020 Dubai, under the patronage of the CSC. The cyber drill aimed to raise awareness about the significance of a systemic approach and training to tackle security issues. The challenge involved cybersecurity professionals from Italian and Emirati national strategic infrastructure companies, universities, and research sectors

7.2. Events involvement

The CSC has been actively involved in a diverse range of national and international events with the goal of advancing the country's cybersecurity agenda. Some of the goals of these events include

- Raising awareness about the latest cybersecurity threats and best practices for addressing them.
- Promoting collaboration among government and private entities to enhance the country's cybersecurity posture
- Showcasing the UAE's cybersecurity capabilities and expertise on a global scale
- Contributing to the development of international cybersecurity standards and frameworks
- Providing a platform for knowledge sharing and networking among cybersecurity professionals
- Building strong partnerships and alliances with other countries and entities to enhance global cybersecurity cooperation

7.3. Achievement

One of the notable achievements of the CSC is the comprehensive coverage of various segments and sectors through its UAE Cyber Pulse initiative. This initiative has successfully covered a wide range of areas, including

- Education
- Energy
- Space
- Medical
- Economy
- Tourism
- Defense
- Nuclear

One of the significant achievements of the CSC is its UAE Cyber Pulse initiative, which has successfully covered a wide range of society members, including

- Parents
- Senior citizens
- Families
- Students
- Employees
- People of Determination

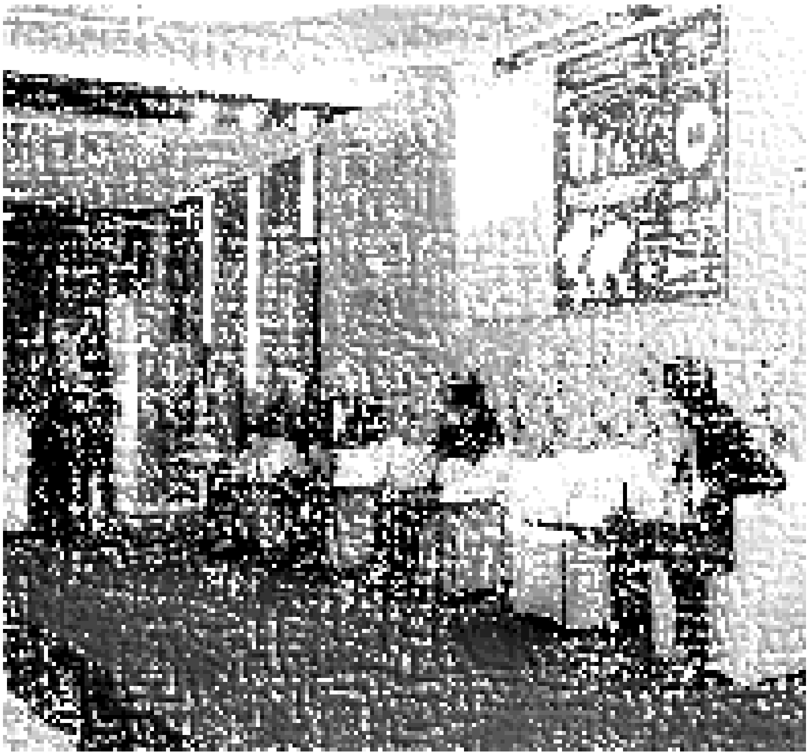
8. 2023 PLANNED ACTIVITIES

The CSC is planning to participate in several global events and summits with the objectives of enhancing international cooperation, sharing best practices, and promoting cyber resilience and safety worldwide such as

- World Government Summit 2023
- Safer Internet Day 2023
- IDEX 2023
- IDC CIO 2023
- World Police Summit 2023

HUAWEI
HUAWEI

الاجتماع الأول للجنة الوزارية للأمن السيبراني بدول مجلس التعاون لدول الخليج العربية
الأمانة العامة ـ الأحد الموافق 23 أكتوبر 2022م



Huawei Tech (UAE) FZ-LLC

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

Following is a summary of key activities that Huawei has been delivering last year as part of the key strategy that prioritise security over business and addressing cybersecurity and privacy challenges and opportunities through technological innovation and open collaboration. This is to foster a better life for all in the future digital world by offering secure and trustworthy products, solutions, and services where personal data is lawfully used and always protected

Help customers manage security risks through technological innovation

- *Continue to build intrinsic security capabilities* in product design. Take 5G base stations, for example; Based on the mobile communications service model, Huawei constantly perform security detection and identity assessment to ensure a quick response. The company deploy functions such as minimum system and continuous security assessment to equip network elements with more effective protection capabilities and helping customers build secure and resilient mobile networks

- *In 2022, Huawei launched the HiSec 3.0 solution*, which uses a three-layer architecture (cloud, local, and edge) and enables integrated defence through the synergy of the cloud, network, and security devices. Huawei's HiSecEngine series, all-in-one intelligent security gateways, are a great fit for businesses seeking to build resilient and secure networks

- *To address customers' pain points in security operations*, Huawei launched the next-generation cloud security operations platform "*Cloud Security Brain*" that allows our customers to greatly improve the efficiency of security operations by quickly managing security events throughout the lifecycle, including alarm discovery, collaborative handling, and event backtracking

- For the HarmonyOS 3 operating system that powers devices, *Huawei have upgraded the Privacy Centre and Security Centre* to make the security status of phones visible to users and help users manage their privacy more effectively. Furthermore, the company has introduced an application control centre to control risky applications appropriately

Consolidate privacy governance to respect and protect user privacy

- In 2022, Huawei released the *Huawei Privacy Governance White Paper* and shared Huawei's privacy governance methods and practices with the industry. The company has also endeavored to protect the rights of data subjects by handling more than 25,000 requests in a timely and effective manner. Moreover, the company has passed over 50 industry-recognized certifications and audits across different countries and business domains, ensuring that the corporate privacy protection policies are well enforced

Strengthening cybersecurity risk management and capability building within Huawei supply chain

- In 2022, Huawei *assessed and managed the cybersecurity risks* of more than 4,000 suppliers worldwide, signed data processing or protection agreements with more than 5,000 suppliers, and managed cross-border data transfers of suppliers to ensure security and privacy compliance

Collaborating with key stakeholders for shared success

- Huawei as the co-chair of OIC-CERT 5G Security Working Group continued its effort by supporting OIC-CERT in accelerating the rollout of 5G among the OIC member countries in a seamless and cost-effective manner. This is done by fostering meetings between the OIC-CERT with local regulators including the Head of Cybersecurity of UAE Government, Vice President for Cybersecurity Affairs, National Telecommunication Regulatory (NTRA) Egypt, hosting adoption workshops, arranged presentation on OIC-CERT 5G Security Framework in major cybersecurity events participated by the country leaders eg. GISEC 2022, Cyber Security Innovation Series Egypt and Tunisia 2022

OIC-CERT
The Organisation of the Islamic Cooperation Computer Emergency Response Team
5G Security Framework
CSIS

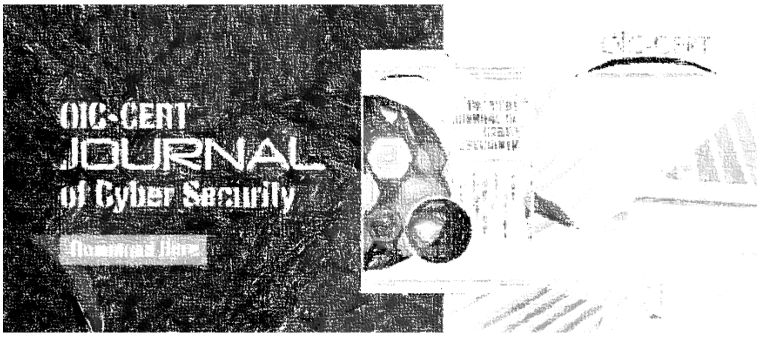
- Huawei also contributed to the 14th OIC-CERT Annual Conference held in conjunction of the Regional Cybersecurity Week in Oman and have done sharing on the implementation of OIC-CERT 5G Security Framework in the exhibition and conference toward the government agencies and regional representatives of FIRST and ITU in the event

الأسبوع الإقليمي للأمن السيبراني ٢٠٢٢م
Regional Cybersecurity Week 2022

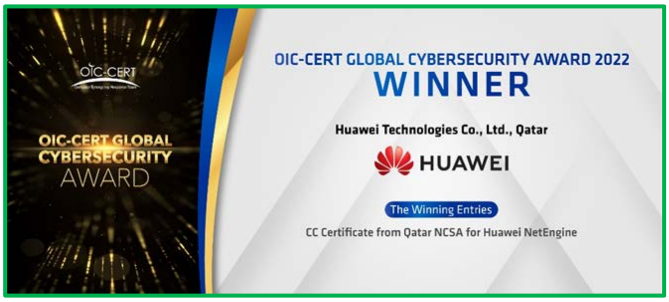
- On Oct 2022, Huawei UAE and (ISC)² UAE Chapter, a non-profit professional cybersecurity organization involved in cybersecurity training and certifications and Huawei signed an MoU to promote cybersecurity awareness, professional training, and certification. The strategic initiative supports knowledge transfer and education towards a robust talent pool for cybersecurity capacity building in the UAE. The joint efforts of an international cybersecurity professional association and a global digital leader constitute a significant step in establishing a more secure, trustworthy, and prosperous cyber oasis in UAE. Both parties will promote cybersecurity awareness, professional training and certification for cybersecurity participants in UAE while facilitating UAE's cybersecurity knowledge transfer and education

1.2. Achievements

In UAE, Huawei deepened the cooperation with the CSC by signing a cybersecurity collaboration MoU and actively contributed to the construction of the local cybersecurity ecosystem, and co-built a cybersecurity think tank and centre of excellence for knowledge sharing and talent cultivation in helping enhance cybersecurity capabilities and awareness within the region. The "*Cyber Plus Innovation*" centre, which focuses on cybersecurity and cyberspace, was launched at Abu Dhabi Polytechnic, a subsidiary of the Abu Dhabi Technical Institute in partnership with the CSC and Huawei, and is dedicated to fostering innovation in the field of cybersecurity. As a result, Huawei received the GITEX Global Cybersecurity Partner Recognition including Cyber Security Leader Award, Cyber Security Company of the Year 2022, and Fortress Cyber Security Award from the CSC in 2022



In Qatar, Huawei Qatar Rep Office has been honoured with the OIC-CERT Global Cybersecurity Award for 2022 through the joint project with Qatar National Cybersecurity Agency (NCSA). The project is to enhance the local public private partnership in the cybersecurity domain and agreed to certify Huawei NetEngine 8000 M14 Router's Software V800R021C00



OIC-CERT GLOBAL CYBERSECURITY AWARD

OIC-CERT GLOBAL CYBERSECURITY AWARD 2022

WINNER

Huawei Technologies Co., Ltd., Qatar

HUAWEI

The Winning Entries

CC Certificate from Qatar NCSA for Huawei NetEngine

In Indonesia, Huawei collaborated with multiple government ministries, including the BSSN, to cultivate cybersecurity talent and improve cybersecurity awareness through training, workshops, and other activities. In 2022, Huawei won the BSSN’s Talent Development Contribution Award.

In Tunisia, Huawei ramped up cooperation with the National Agency for Computer Security, Tunisia, and made active contributions to knowledge sharing, talent cultivation, and ecosystem development. In 2022, Huawei won the ICT Industry and Talent

Development Award by the Prime Minister of Tunisia

In Thailand, Huawei worked with the NCSA Thailand on activities like the Thailand Cyber Security Week and various cybersecurity competitions that help identify local talent and improve cyber security awareness. The company also delivered in-depth training on cybersecurity technologies and standards for a wide array of local organizations and talent through e-lab, a dedicated online learning platform. As a result, Huawei was awarded the Thailand Cybersecurity Excellence Award by the Thai Prime Minister H.E. General Prayut Chan-o-cha

2. ABOUT ORGANIZATION / AGENCY

2.1. Introduction

Huawei is a leading global provider of information and communications technology (**ICT**) infrastructure and smart devices. The company has more than 194,000 employees, and operates in more than 170 countries and regions, serving more than three billion people around the world

The vision and mission is to bring digital technology to every person, home, and organization for a fully connected, intelligent world. To this end, Huawei will drive ubiquitous connectivity and promote equal access to networks; bring cloud and artificial intelligence to all four corners of the earth to provide superior computing power where needed, when needed; build digital platforms to help all industries and organizations become more agile, efficient, and dynamic; redefine user experience with Artificial Intelligence (**AI**), making it more personalized for people in all aspects of their life, whether they're at home, in the office, or on the go.

Huawei has operated in the Middle East region for over 20 years now, with Bahrain as the regional headquarters and the UAE as the MEA business centre, with Dubai as one of the six global cybersecurity centres. 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. Subsequently Huawei published the first cybersecurity white paper in 2012, the second one in 2013, the third white paper in 2014, and a fourth in 2016 and our most recent position paper in 2019

2.2. Establishment

1987

2.3. Resources

Huawei Trust Centre (*https://www.huawei.com/en/trust-center*)

Huawei Cloud Trustworthiness Knowledge Base (*https://www.huaweicloud.com/intl/en-us/securecenter/resource.html*)

2.4. Constituency

Huawei's customers in the global ICT eco-system are in over 170 countries and regions where Huawei provide products, services and end-to-end solutions to carrier network clients, enterprise customers, government, and end-user consumers supporting them in their digital transformation journey

3. 2023 PLANNED ACTIVITIES

- Deepen the cooperation and development with industry stakeholders

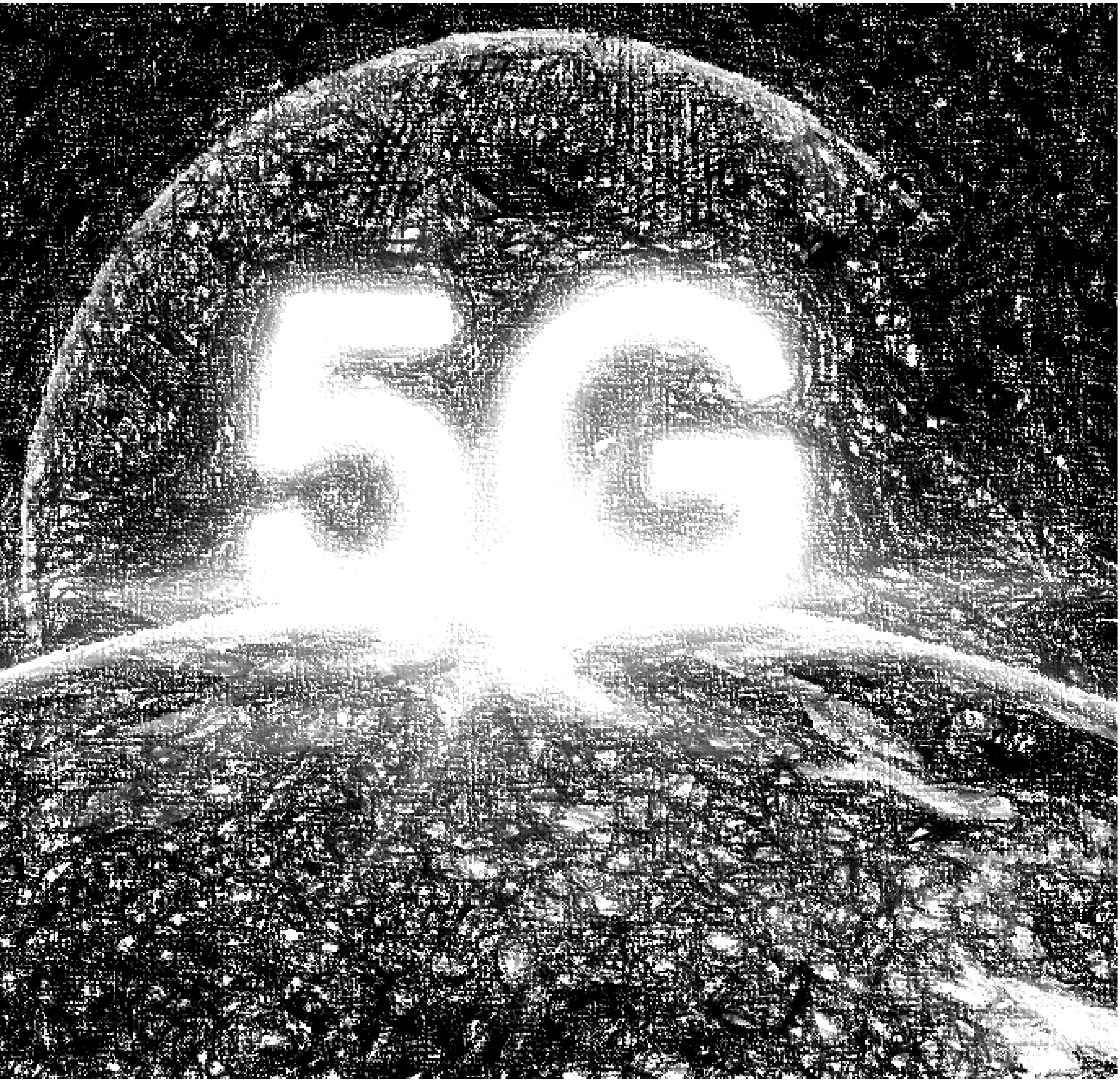
  - *OIC-CERT*: continue to optimize the rollout of OIC-CERT 5G Security Framework and support the establishment of the OIC-CERT Cloud Security Working Group. Huawei will contribute by launching the Cloud Security Whitepaper in Middle East region that align with the objectives of the OIC-CERT Cloud Security Working Group
  - *Other Industry organizations*: Collaboration with leading cybersecurity associations including (ISC)² UAE Chapter, Cloud Security Alliances (CSA) UAE Chapter and help create and maintain a strong and vibrant cybersecurity local ecosystem to position the UAE as a globally trusted digital hub

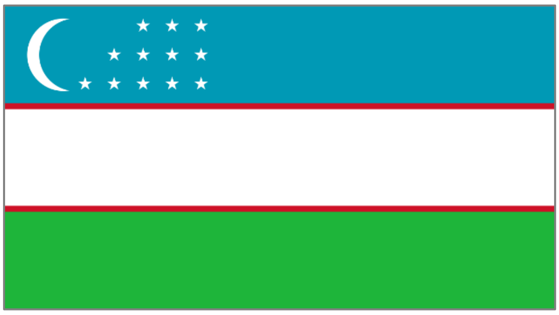
- Continuously enhancing secure and trustworthy delivery and service operations

Organizing cybersecurity training and certification for partners and contractors to continuously improve cybersecurity awareness and capabilities. Moreover, Huawei actively communicated with industry stakeholders to jointly build cybersecurity capabilities in response to mounting cybersecurity challenges. Huawei has continued to optimize the presence of global service centres to ensure more flexible service delivery. Meanwhile, the company organized the Network Safety Day campaign with customers to identify and mitigate risks on live networks, strengthen cybersecurity awareness, enhance cyber resilience, and support secure and stable network operations

- Increasing investment in independent third-party verification

In 2022, Huawei obtained more than 30 internationally recognized cybersecurity certificates. The company will continue the cooperation with industry-recognized certification bodies to test the cybersecurity capabilities of Huawei products against international standards and best practices and providing customers with internationally recognized security assurance. We continued to encourage employees to pursue external professional certification programs and, to date, more than 2,000 employees have obtained industry-recognized certifications such as the CISSP, Certificate of Cloud Security Knowledge (CCSK), and Certified Information Privacy Manager (CIPM). Huawei has also planned and developed new cybersecurity enablement courses and exams





UZBEKISTAN

Uzbekistan Computer Emergency Response Team (UzCERT)

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

The team faced many interesting challenges in 2022, which was dealt with. UzCERT started the journey by becoming a member of FIRST. The team also deployed the Web Application Firewall, in collaboration with partners, which helps to prevent several types of attacks

1.2. Achievements

- Relevant organizational and technical measures were done as part of the membership requirement for FIRST
- 4 510 318 repelled cyber attacks on websites
- 730 vulnerabilities found
- 345 technical assistance provided to organizations
- 201 examinations carried out
- 251 incident responses

2. ABOUT THE ORGANIZATION/ AGENCY

2.1. Introduction

The Uzbekistan Computer Emergency Response Team - UZCERT service, act as a structural subdivision of the State Unitary Enterprise "Cybersecurity Centre". It focuses on cooperation and interaction with operators and providers, law enforcement agencies, as well as users of the national segment of the Internet, in providing the necessary support in responding to cybersecurity incidents. The UZCERT service conducts the necessary analysis of artifacts in case of incidents, establishes the causes and consequences of the incident, and prepares recommendations for effectively counteracting virus and hacker attacks

Given the cross-border nature of cybersecurity threats and incidents, UZCERT aimed at broadening cooperation with foreign partners in order to harness the capabilities and experience of the global community in combating cyberthreats and cybercrimes

This approach resulted to a positive dynamics of information on cybersecurity threats and incidents, including through continuous training of employees in the field of computer forensics, malware analysis and the best global practices for responding to cybersecurity threats and incidents

2.2. Establishment

Increased attention to the issues and problems of cybersecurity led to the approval of the Strategy for the further development of the capabilities of the Republic of Uzbekistan. The aim is the implementation of five (5) major strategic initiatives, among which the priority to ensure security and cybersecurity (*Resolution of the President of the Republic of Uzbekistan dated February 7, 2017*)

The tasks for implementing the state initiatives in the field of information protection and cybersecurity are entrusted to the Centre for Information Security, established in 2013 and in 2019, by decision of the government, it was transformed into the State Unitary Enterprise Cybersecurity Centre. The upgraded entity has an increase role as the executor of state policy in the fields of information and cybersecurity

2.3. Resources

Government

2.4. Constituency

UZCERT assists in ensuring cybersecurity at the national segment of the Internet of the Republic of Uzbekistan

3. ACTIVITIES AND OPERATION

3.1. Events organized by the organization/ agency

The State Unitary Enterprise "Cybersecurity Center" on an ongoing basis conducts seminars and training courses that address issues of information protection and cybersecurity for authorized employees of state bodies and institutions of the Republic of Uzbekistan

3.2. Events involvement

- Participation in the international forum on practical security "*Positive Hack Days*".
- Participation in the annual conference on the topic: "*Security Identification 2022*"
- Participation in the FIRST 2022 Conference: "*Neart Le Chéile: Strength Together*"
- participation in the ITU Interregional Cybersecurity Exercise for the CIS region and the Arab States
- World Radiocommunication Conference 2022 (ITU)
- 7th CAMP Annual Meeting
- Building social resilience by raising public awareness on cyber threats and strengthening the role of cybersecurity education by Organization for Security and Co-operation in Europe (OSCE)
- Participation in the 10th OIC-CERT General Meeting and the 14th Annual Conference 2022, which was held in conjunction with the 10th Regional Cyber Security Summit and the FIRST and ITU-ARCC Regional Symposium 2022
- Participation in the 7th international conference - exhibition in the field of national security and cybersecurity "*Israel. HLS&CYBER 2022*"

- Participation in the delegation for the development of digital services and establishing cooperation with advanced technological experience of Sberbank PJSC (*The composition of the delegation of the Republic of Uzbekistan was headed by the Minister for the Development of Information Technologies and Communications Sh.Kh. Shermatov*)
- Organization of "*University CTF Challenge*" held among university students and Cybersecurity Centre specialists
- Participation in CyberDrills

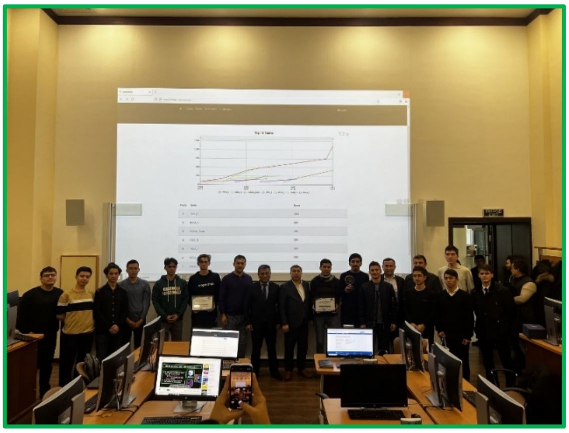
3.3. Achievement

A set of measures has been implemented for the interaction of the Shanghai Cooperation Organisation (**SCO**) member states to ensure international information security

4. 2023 PLANNED ACTIVITIES

The following activities are planned for 2023

- Become a full-member of FIRST
- Request Tracker for Incident Response (RTIR) system implementation
- Improvement of activities (according to SIM3)
- Improvement of the quality of provision of services
- Advanced training for specialists and obtaining CEH and Computer Hacking Forensic Investigator (CHFI) certifications
- Host the Cyber Security Summit - Central Eurasia 2023 conference and showcase



YEMEN

Smart Security Solutions (SMARTSEC)

Dr. Abdulrahman Ahmad Abdu Muthana

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- Cyber Security Awareness Training in a few of universities
- Penetration testing for several financial companies
- Implementing secure networks for different companies and agencies
- Ransomware Analysis
- Fraud Investigations in local financial company
- Cybersecurity training for professionals

1.2. Achievements

- Establishment of special Cybersecurity courses for non IT staff
- Penetration Testing for several local financial companies
- Investment on AI research in Cybersecurity
- Analyzing Phobos ransomware virus

2. ABOUT THE ORGANIZATION / AGENCY

2.1. Introduction

Smart Security Solutions Company (**SMARTSEC**) is the first company in Yemen to provide information security training, consultancy, and research

2.2. Establishment

SMARTSEC was established in Oct 2010 by Dr.Abdulraman Muthana and a group of information security professionals

2.3. Resources

SMARTSEC includes a number of information security professionals and researchers. The company has 2 training labs equipped with facilities in addition to a research lab

2.4. Constituency

Information security fields

3. ACTIVITIES AND OPERATIONS

3.1. Events organized by the organization/ agency

- Cybersecurity awareness training for universities
- Seminars on cybersecurity careers
- Cybersecurity training for certification preparation

3.2. Events involvement

- Information security training
- Information security awareness programs
- Ransomware incidents analysis
- Fraud investigations in local financial companies

3.3. Achievements

- Training a number of cybersecurity courses
- Establishment of special cybersecurity courses for non IT staff
- Ransomware virus investigations

4. 2023 PLANNED ACTIVITIES

- SMARTSEC aims to invest more in AI researches in cybersecurity and malware analysis
- More engagement in helping organizations in Yemen to implement the ISO 27000 (ISMS) Standard

SINGAPORE

Group IB (CERT-IB)

1. HIGHLIGHTS OF 2022

1.1. Summary of Major Activities

- 19 years of operation since the establishment of Group-IB
- 70000+ hours of hands-on Incident Response
- 1300+ successful investigations of hi-tech cybercrime cases
- Digital Risk Summit' 2022

- Operation Delilah, joint investigation with Interpol
- Operation Falcon II, joint investigation with Interpol
- Group-IB supports CERTFin to guard Italian financial sector
- Annual Ransomware report
- OldGremlin ransomware report
- Report "*OPERA1ER. Playing God without permission*," in collaboration with the researchers from Orange CERT Coordination Centre
- Africa Cyber Surge Operation: Group-IB assists INTERPOL-led operation to combat cybercrime
- Technical research "*Godfather, an Android banking Trojan*"

1.2. Achievements

- Global Analytical Report inclusion: Gartner, Frost & Sullivan, GIGAOM, Aite Novarica
- Group-IB's products and services honoured with Gold by the Cybersecurity Excellence Award 2022 include:
  - o Email Security Group-IB Atmosphere
  - o Advanced Persistent Threat Protection (APT) Threat Hunting Framework (THF)
  - o Anti Malware THF Polygon
  - o Anti phishing Threat Hunting Framework & Digital Risk Protection
  - o Forensics Digital Forensics
  - o Phishing Detection and Response (PDR) Digital Risk Protection
  - o Cyber Threat Intelligence Threat Intelligence & Attribution
- Jennifer Soh, Senior Cyber Investigation Specialist, and Kristina Ivanova, Deputy Head of the Group-

IB's Cyber Investigations team in Singapore, have been featured in the list of Top 30 Women in Security ASEAN Region

2. ABOUT ORGANIZATION / AGENCY

2.1. Introduction

CERT-GIB 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

Aside from being an OIC-CERT partner, CERT-GIB is an accredited member of Trusted Introducer, a member of FIRST, and a strategic partner of the International Multilateral Partnership Against Cyber Threats (IMPACT)

2.2. Establishment

March 10, 2011

2.3. Resources

Human intelligence

More than 60 employees working around the clock to ensure everyone who needs help can get it

CERT-GIB works closely with Group-IB's Digital Forensics Laboratory, and Threat Intelligence & Attribution and Investigations teams

Proprietary technology

Group-IB Threat Hunting Framework allows CERT-GIB experts to manage incidents effectively and efficiently and reduce time spent on incident analysis

CERT-GIB operations are enhanced with data collected by Group-IB Threat Intelligence & Attribution

Malware analysis further reinforces CERT-GIB's capabilities, as it allows experts to prevent severe data breaches and network infections and detect vulnerabilities within the perimeter

Combined, Group-IB technological capabilities include

- Internal and external threat hunting
- Graph analysis
- Data storage
- Correlation and attribution
- Event analysis

Unmatched expertise

CERT-GIB 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 combined technological capabilities and human intelligence means the company is always aware of cyber criminals’ latest tools, TTPs, and movements

International cooperation

CERT-GIB is part of a global network of CERTs that actively engages in information and intelligence sharing

CERT-GIB is also actively collaborating with top-level Russian domains to block dangerous websites

2.4. Constituency

Service Provider Customer Base

CERT-GIB's constituency includes organizations from the media, law enforcement agencies, government sector, ISP, private sector and CII

3. ACTIVITIES AND OPERATION

3.1. Events organized by the organization/ agency

Events

Digital Risk Summit

Webinar

- Detecting MaliBot with a Fraud Protecting solution
- Ransomware Insights 2021-2022
- Fraud Intelligence Series 2022
- APAC-Fraud Hunting Day Act I
- APAC-Fraud Hunting Day Act II
- Arms race: Fraudster use of neural network technology
- OPERA1ER : *Comment Des Millions De Dollars Ont Été Dérobés À Des Banques*
- OPERA1ER: How Millions Were Stolen From Banks
- Intelligence briefing series
- Introducting Unified Risk Platform
- Having doubts? Detonate! Malware detonation for threat analysts
- How to comply with SAMA CTI framework
- Implement a Future-Proof Cyber Education Strategy

3.2. Events involvement

Events in Europe

- Amsterdam 2022 FIRST Technical Colloquium
- Group-IB Partner Universe (Distributor Boothcamp)
- BotConf
- Ready for IT
- Reseller event - Ingram Micro Poland
- HackInBo
- Risk Conference
- Annual e-Crime & Cybersecurity Congress
- Money 2020
- FIC
- FIRSTCON22
- HSD Café: Cybersecurity in FinTech
- Abbakan Roadshow
- Forum IT: Cyberattacken erkennen und abwehren
- FS-ISAC
- Cyber Defnse Summit
- Forum Banca
- BankInfo
- Cyber Act Forum
- TechHosted
- Les Assises - Business Lunch by Abbakan
- One Conference
- Ingram Micro Security Summit

Events in Middle East and Africa

- GISEC 2022
- Group-IB Incident Response Game
- Future of Data Centers'22
- Africa Pay and ID Expo, Morocco
- Africa Cyber Defence forum
- MENA ISC'22
- GITEX'22
- Group-IB Fraud Day, Saudi Arabia
- Black Hat 2022
- Gartner SRM Summit with CyberKnight
- Partner Universe 2022
- LEAP
- Cyber Security Summit, Kenya

Events in APAC

- Cyber Security Asia, CSA 2022
- Security bootcamp 2022
- IT Conference 2022 with Smartez
- Australian Cyber Conference 2022 - Melbourne
- GovWare 2022
- MRC Singapore - Asia-Pacific Payments and Fraud Conference
- Advancing Cyber Insights with Group-IB - ASM Reseller Day with Tech Data

- Secure 2023 - Thailand - Nforce
- NASSCOM-DSCI Annual Information Security Summit
- SINCON Reloaded
- 22nd Next Generation Security Vision 2023 Seminar & Exhibition
- Australian Cyber Conference, Canberra

3.3. Achievement

Global Analytical report

- Aite Novarica

  Attack Surface Management Avoiding Device Whack-A-MolE *https://aite-novarica.com/report/attack-surface-management-avoiding-device-whack-mole*
- Incident Response Retainer Services: Responding to the Scene of the Crime *https://aite-novarica.com/webinar/incident-response-retainer-services-responding-scene-crime*

Frost & Sullivan

- Frost Radar™: External Risk Mitigation and Management (ERMM) Platforms, 2022
- Global Fraud Detection & Prevention (FDP) Market Study *https://www.frost.com/news/enterprise-security-concerns-drive-global-demand-for-fraud-detection-prevention -solutions/*
- Frost Radar: Cyber Threat intelligence

Gartner

- Market Guide for Digital Forensics and Incident Response Retainer Services
- Emerging Tech: Adoption Growth Insights in Digital Risk Protection Services
- Market Guide for Online Fraud Detection

GIGAOM

- GigaOm Radar for Attack Surface Management
- GigaOm: Radar for Threat Intelligence Solutions

Group-IB's products and services honored with Gold by the Cybersecurity Excellence Award 2022 include:

- Email Security Group-IB Atmosphere
- Advanced Persistent Threat Protection (APT) Threat Hunting Framework (THF)
- Anti Malware Threat Hunting Framework Polygon
- Anti phishing Threat Hunting Framework & Digital Risk Protection
- Digital Forensics
- Phishing Detection and Response (PDR) Digital Risk Protection
- Cyber Threat Intelligence & Attribution

4. 2023 PLANNED ACTIVITIES

Europe

- Risk Conference
- FS-ISAC
- Cybertech Europe
- StrategyDays IT Security
- ISMS Forum
- SIGMA

APAC

- IEC Smart Banking - Vietnam
- GovWare - Singapore
- Australian Cyber Conference
- CRESTCon Australia

Middle East and Africa

- IDC CIO Summit, South Africa
- MENA ISC, Saudi Arabia
- Black Hat, Saudi Arabia
- GISEC 2024

OIC-CERT
THE ORGANIZATION OF THE ISLAMIC COOPERATION - COMPUTER EMERGENCY RESPONSE TEAM
5G SECURITY FRAMEWORK
WORKING GROUP

OIC-CERT

Computer Emergency Response Team

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