OIC-CERT

Computer Emergency Response Team

OIC-CERT 2023

ANNUAL REPORT

Organization of the Islamic Cooperation
Computer Emergency Response Team

Table of Contents

About OIC-CERT

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

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

VISION

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

MISSION

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

OBJECTIVES

Strengthening the relationship of CERTs among the OIC Member countries, OIC-CERT partners, and other stakeholders in the OIC community

Encouraging the sharing of cybersecurity experience and information

Preventing and reducing cyber-crimes by harmonizing cybersecurity policies, laws, and regulations

Building cybersecurity capabilities and awareness amongst the OIC-CERT member countries

Promoting collaborative research, development, and innovation in cybersecurity

Promoting international cooperation with international cybersecurity organizations

Assisting the OIC-CERT member countries in establishing and developing national CERTs

MEMBERSHIP

As of Dec 2023, the OIC-CERT has a network and strategic collaboration with 63 members from 28 OIC countries. This alliance is further supported through the presence of six (6) Commercial

Members, five (5) Professional Members, three (3) Fellow Member, one (1) Affiliate Member, and 1 Honorary Member

Full Members

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

General Members

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

1. Azerbaijan
   - Azerbaijan Cybersecurity Organizations Association (ACOA)
2. Bangladesh
   - BangladeshCERT
   - Bangladesh Computer Emergency Response Team (bdCERT)
3. 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)
4. Jordan
   - Unit of Financial Computer Emergency Response Team (JoFin-CERT)
5. Kazakhstan
   - Center for Analysis and Investigation of Cyber-Attacks (CAICA)
6. Kyrgyzstan
   - Computer Emergency Response Team (CERT.ICT KG)
7. Malaysia
   - Universiti Teknikal Malaysia Melaka (UTeM)
8. Pakistan
   - Pakistan Information Security Association (PISA-CERT)
9. Türkiye
   - Turkey Cyber Security Incident Response Team (TR-CSIRT)
10. Uganda
    - Uganda Computer Emergency Response Team (UG-CERT)
11. Uzbekistan
    - Inha University in Tashkent

Affiliate Members

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

The United States
- Team Cymru

Commercial Members

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

1. Brunei Darussalam
   - ITPSS Sdn. Bhd
2. Malaysia
   - FNS (M) Sdn. Bhd
3. Singapore
   - CERT-GIB
4. Türkiye
   - Turkcell CDC
   - Turkish Airlines CERT (THY-CERT)
5. UAE
   - Huawei (HWT)

Professional Members

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

1. Malaysia
   - Abdul Fattah Mohamed Yatim - *Teknimuda (M) Sdn Bhd*
   - Hatim Mohammad Tahir
   - Prof. Dr. Rabiah Ahmad - *Universiti Tun Hussein Onn Malaysia*
   - Dr. Sofia Najwa Ramli – *Universiti Tun Hussein Onn Malaysia*
2. Yemen
   - Dr. Abdulrahman Ahmad Abdul Muthana - *Smart Security Solutions*

Fellow Members

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

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

Honorary Members

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

Saudi Arabia
   - Organisation of the Islamic Cooperation

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

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

1 AZERBAIJAN

Azerbaijan Government CERT

1.1 ABOUT THE ORGANIZATION

1.1.1 Introduction

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

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

1.1.2 Establishment

20 Apr 2008

1.1.3 Resources

Official web sites:

https://cert.gov.az/
https://scis.gov.az/

Social media links:

https://youtube.com/@certgovaz
https://facebook.com/certgovaz
https://twitter.com/certgovaz
https://telegram.me/certgovaz
https://linkedin.com/company/certgovaz

1.1.4 Constituency

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

1.2 HIGHLIGHTS OF 2023

1.2.1 Events organized by the organization / agency

7 Feb 2023 Baku, Azerbaijan - The 1st Summit of CISOs of the state institutions dedicated to Safer Internet Day

1st Summit of CISO of the State Institution

1 May 2023 Baku, Azerbaijan - Webinar for engineers and programmers of the Ministry of Communications and New Technologies of the Nakhchivan AR of the Azerbaijan Republic

Webinar for Engineer & Programmer for Ministry of Communications & New Technologies

21-23 Sep 2023 Baku, Azerbaijan - The 2nd Summit of CISOs of the state institutions and Digital Economies and Cybersecurity Conference devoted to the International Cyber Security Days

2nd Summit of CISO of State Institution

17 Oct 2023 Baku, Azerbaijan - The 30th meeting of the CIS Coordination Council for Government Communications

30th Meeting of CIS Coordination Council for Govt Communications

26-27 Oct 2023 Baku, Azerbaijan - Critical Infrastructure Defence Challenge (**CIDC-2023**) conference, which includes a virtual war competition with the simulation of cyber-attacks, an exhibition of cyber solutions, several masterclass trainings under the Hack the Future program, workshops, and quizzes with gifts for visitors. Official website: *https://cidc.gov.az/*

CII Defence Challenge

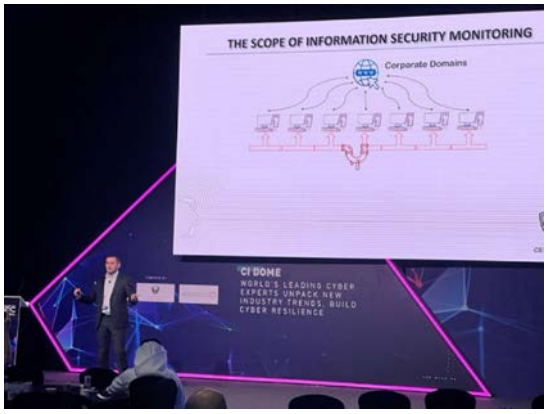
1.2.2 Events involvement

13 Mar 2023 - The event on Technologies for sustainable development:

'Technologies and Cloud Solutions of the 4th Industrial Revolution' organized by the Analysis and Coordination Centre of the Fourth Industrial Revolution under the Ministry of Economy, Baku, Azerbaijan

Technologies for Sustainable Development 4th Industrial Revolution

14-16 Mar 2023 Dubai, UAE – The Gulf Information Security Expo & Conference 2023 (**GISEC** 2023) Global cybersecurity exhibition and conference hosted by the Cyber Security Council (**CSC**), UAE



GISEC 2023 Global

25 Apr 2023 Bucharest, Romania - International Conference on Cyber Diplomacy

International Conference on Cyber Diplomacy

19–23 Jun 2023 Vienna, Austria - International conference on Computer Security in the Nuclear World: Security for Safety held by the International Atomic Energy Agency

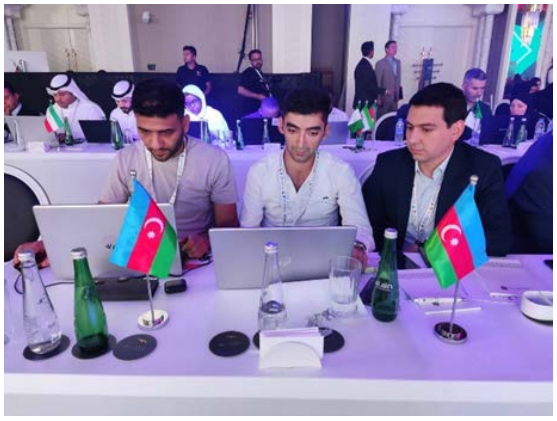
13-15 Sep 2023 Almaty, Kazakhstan - KazHackStan – Turan 2023 Conference

KazHackStan - Turan 2023

3-4 Oct 2023 Tashkent, Uzbekistan - Central Eurasian Cyber Security Summit

Central Eurasian Cyber Security Summit

9-12 Oct 2023 Abu Dhabi, UAE - Regional Cybersecurity Week 2023



Regional Cybersecurity Week 2023

9-10 Nov 2023 Ashgabat, Turkmenistan - TürkmenTEL-2023 International Exhibition and Conference

1.3 ACHIEVEMENTS

Launched the new Information Security Calendar 2023 project with the aim of strengthening information security habits and raising awareness in state institutions

A new platform called *share.gov.az* was put into use to strengthen information security in the state institutions and eliminate dependence on local and foreign disk carriers that can cause information leakage

Released '*Tusi Paleon*' - the first lightweight malware forensics tool in Azerbaijan

Organized masterclass events by our experts to increase the theoretical, scientific and practical knowledge level of students studying in the field of information security at a number of local universities

Conducted an assessment test and awarded scholarships to distinguished students of the Azerbaijan State Technical University

In developing international relations, Memorandum of Understandings (**MoU**s) were signed with several organizations as follows:

- TÜBİTAK Informatics and Information Security Research Center (BİLGEM) of Republic of Türkiye
- The National Cyber Security Directorate of Romania
- The State Unitary Enterprise Cyber Security Center of the Republic of Uzbekistan
- Turkmenaragatnashyk, agency of the Republic of Turkmenistan
- State Technical Service JSC of the Republic of Kazakhstan

Recorded and handled 911M incidents by the next-generation firewall (**NGFW**), 7.5M malware by centralized endpoint protection platform and 104K malicious documents with the special sandbox

Prevented specifically targeted Advance Persistence Threats (**APT**) cyberattacks by identifying and blocking 1,162 IOCs

Blocked 186 impersonated state domains (*.*gov.az*) detected by various computer telephony integration (**CTI**) tools

Processed a total of 27.8M e-mails through the State E-mail Service and blocked 2.8M of them due to their malicious content. Currently, 30K employees of state institutions (on more than 549 domain names) use the e-mail service

Provided 695 audit/ penetration test (*pentest*) for required government entities

Received 7,067 requests/ tickets from state institutions over the Electronic Request System and implemented the necessary security measures

Published 3 editions of the Information Security Journals for the government bodies

Actively participated in several TV programs and media news for public awareness

Information Security Journal

1.4 2024 PLANNED ACTIVITIES

Continue the Information Security Calendar – 2024 project to strengthen information security habits and awareness

Organize meetings with CISOs of the state institutions on a semi-annual basis

Redesign and upgrade the OIC-CERT membership portal with new features like the teams' communication and information sharing capabilities

Introduce a new cybersecurity awareness platform for the use of OIC-CERT members, which is also intended to be implemented in the state institutions of Azerbaijan as a continuation of the cyber hygiene project and includes the Learning Management System (**LMS**) and phishing simulation capabilities

Organization of the first International Cyber Diplomacy Conference in Azerbaijan

Participate in the Azerbaijan Defence Exhibition (**ADEX**) and Securex Caspian exhibitions to be held in Sep 2024

Launch a Graphical User Interface (**GUI**) version of '*Tusi Paleon*' tool and new remote Indicator of Compromise (**IOC**) scanner called '*10C Hunter*'

Continue the regular issues of the Information Security Journals

Continue collaboration with CERTs internationally

Regional Cybersecurity Week 2023

1st Summit of CISO for State Institutions

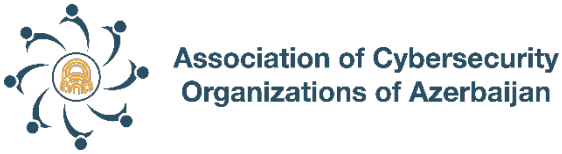
Turkmen TEL-2023

2nd Summit of CISO for State Institutions

Central Eurasian Cyber Security Summit

Information Security Journal published in 2023

Association of Cybersecurity Organizations of Azerbaijan



1.1 ABOUT THE ORGANIZATION

1.1.1 Introduction

The primary objective of the Association of Cybersecurity Organizations of Azerbaijan (**ACOA**) is to unite stakeholders in the cybersecurity sector and collaboratively work towards establishing a robust cybersecurity ecosystem for the country. ACOA's primary objectives are to enhance the cybersecurity ecosystem in the country, coordinate measures implemented in the field of cybersecurity (hereinafter referred to as the relevant field) and offer support for the development of this crucial domain. ACOA, whether independently or through collaboration with its members, specialized companies, and experts, engages in scientific research, certification, technical expertise, education, and consulting services across the domains of cybersecurity and various information technologies

1.1.2 Establishment

ACOA was officially registered on 19 Apr 2022, serves as a cohesive platform for experts, companies, and organizations within the cybersecurity and information communication technologies sectors. It aims to provide a secure vision for the future

1.1.3 Resources

Professionals specializing in information technologies, particularly in the field of cybersecurity, can join ACOA as physical members and contribute as experts. State and private enterprises, international organizations, official representations of companies in the country, public organizations, and associations are eligible to become legal members of ACOA

1.1.4 Constituency

ACOA committees are formally organized to address various information security subjects, sectors, and technology domains. Comprising voluntary participants, these committees serve as forums where members share information about their respective fields, discuss issues, and collaboratively prepare proposals, recommendations, and documents. The decisions and recommendations put forward by the committees significantly influence the activities of ACOA, forming the basis for proposals presented by the organization. ACOA's legal body representatives and independent experts actively participate

in the committee's activities. To join the committee, individuals can submit applications through the web cabinet or send official emails to the relevant legal personnel who are ACOA members. The committees operate for a one-year term, with the number of participants determined by ACOA. Each committee includes a secretary, a chief secretary, and other members. During the acceptance of new members, priority is given to the members involved in specific field. The election of the Chairman and Chief Secretary occurs annually, with no restrictions on the re-election of the same individuals

1.2 HIGHLIGHTS OF 2023

1.2.1 Summary of Major Activities

In 2023, ACOA hosted over 30 events, including forums, conferences, seminars, competitions, and training sessions, engaging more than 4,000 participants. In addition, ACOA has embarked on international outreach efforts, with delegations visiting five countries - Turkey, Israel, Korea, Kazakhstan, and Uzbekistan

ACOA also has undertaken more than 10 research and development projects. Apart from promoting cybersecurity awareness in educational settings, ACOA established cybersecurity corners in STEAM[1] centres located in Barda, Ganja, Shirvan, and Lankaran

1.2.2 Achievements

ACOA conducted over 90 meetings to enhance cooperation and established cyber clubs in 15 higher education institutions to foster effective relationships within the academia

Due to ACOA's accurate portrayal of the systematic cybersecurity measures implemented in Azerbaijan in 2023, reflected in relevant metrics, Azerbaijan has improved its ranking by 36 points and advanced its position from 86th to 50th place in the rating table of the National Cybersecurity Index, which assessed 176 countries (*https://ncsi.ega.ee/*)

Two Memorandum of Cooperation agreements were signed with the higher education institutions

1.3 ACTIVITIES & OPERATIONS

1.3.1 Events Organized

Cyber Star National Capture the Flag (**CTF**) League - organized by ACOA - AKTA for the purpose of conducting competitions on cybersecurity *https://akta.az/news/kiber-ulduz-milli-ctf-liqasina-qeydiyyat-basladi*

CTF Competition "International Security Day

[1] Science, Technology, Engineering, Art, Mathematics

6 Apr 2023 - Seminar on Critical Information Infrastructure Security: National and International Aspects with the participation from relevant institutions, companies, and international experts, ACOA and the partnership of Softprom and Cisco *https://akta.az/news/kritik-informasiya-infrastrukturunun-tehluekesizliyi-milli-ve-beynelxalq-aspektler-adli-seminar-kecirilib*

31 Mar to 7 Apr 2023- visits to STEAM centres located in Ganja, Barda, Shirvan, and Lankaran within the framework of the project Education on Cybersecurity in General Educational Institutions implemented by ACOA with the financial support of the Ministry of Science and Education *https://akta.az/news/gence-berde-sirvan-ve-lenkeranda-yerlesen-steam-merkezlerine-seferler-teskil-olunub*

14 Apr 2023 - Cyber Security Platform (**KTP**), Baku Youth Center (**BGM**), and AKTA jointly organized the cybersecurity personal development and training program '*Cyber Cafe – 2023*'. The event, held at the BKM, was sponsored by the companies Aselsan Baku, Allsafe Cybersecurity, OzGadabey, and with the technical and organizational support of Azerbaijan Technical University, Creative Developers Club, and the company Pringberg *https://akta.az/news/bakida-kiber-kafe-2023-kibertehluekesizlik-sexsi-inkisaf-ve-telim-proqrami-adli-tedbir-kecirilib*

15 Apr 2023 -, a CTF competition organized by ACOA at the Baku Higher Oil School of SOCAR[2] with the participation of teenagers aged 12-17. The companies Interprobe and UnifyBytes acted as the technical organizers of the competition with the support of the Ministry of Science and Education of the Republic of Azerbaijan and Cyberpoint as part of the Cybersecurity Awareness Project in Public Educational Institutions *https://akta.az/news/kiber-ulduz-kibertehluekesizlik-uezre-ctf-yarisi-ugurla-bas-tutub*

31 May 2023 - The 2nd National Cyber Security Forum dedicated to the 100th anniversary of National Leader Heydar Aliyev held and organized by ACOA and the main sponsorship of A2Z Technologies. Discussions were conducted involving leaders and experts from related state institutions and private companies/ organizations *https://akta.az/news/31-may-2023-cue-il-tarixinde-uemummilli-lider-heyder-eliyevin-100-illiyine-hesr-olunmus-2-ci-milli-kibertehluekesiz lik -forumu-kecirildi*

12 Jun 2023 – ACOA organized a scientific-practical seminar on cryptography at the Azerbaijan Technical University with the participation of relevant experts from 14 higher education institutions. The forum has experts in the field discussing,

[2] State Oil Company of the Republic of Azerbaijan

among others, the importance of cryptography in the context of cybersecurity, innovations in the field of cryptography, the role of cryptography in blockchain technologies, cryptographic security protocols
https://akta.az/news/12-iyun-2023-cue-il-tarixinde-kriptoqrafiya-uezre-elmi-praktiki-seminar-heyata-kecirildi

12 Jun 2023 – ACOA organize a training, in English, in the field of cryptography. This started at Azerbaijan Technical University by foreign experts (with the support of ACOA member company Unifybytes (Turkey)) for students studying information security at the higher learning institutions of the country
https://akta.az/news/kriptoqrafiya-sahesinde-telimlere-start-verildi

24 July 2023 - the opening event of the International Summer School 'Cyber Summer School – 2023' for school children and teenagers aged 12-16 years held at the Bilgah Recreation Center of the State Security Service. Organized by ACOA, sponsored by Azerconnect LLC, Caspel, Cyberpoint, Techpro DC, and Huawei Technologies, in partnership with Gesco, A2Z Technologies, CISCO and Azerobot companies. The presentations and speeches from the relevant state institutions, embassies of foreign countries operating in the country, as well as senior officials of higher education institutions were heard at Baku Higher Oil School attended by teenagers and their parents lasted until 30 Jul. In addition, the participants of the opening event got acquainted with technological solutions and services from companies such as Caspel, Cyberpoint, Techpro DC, Huawei, A2Z Technologies, Cisco, and Azerobot companies
https://akta.az/news/dtx-nin-bilgeh-istirahet-merkezinde-yay-mektebinin-acilisi-oldu

Within the framework of the project Fighting Fake News in Cyberspace organized by ACOA, trainings for media representatives have been successfully conducted. The aim of the trainings is to raise awareness among media representatives about the concept of fake news and the fight against them, as well as raising awareness of the ways and mechanisms of fighting disinformation and fake news
https://akta.az/news/kibermekanda-saxta-xeberlerle-muebarizenin-aparilmasi-layihesi-cercivesinde-telimler-davam-edir

15 Oct 2023 - Cybersecurity Trends Seminar was successfully held during the Cybersecurity Awareness Month. Eighty (80) people participated in the seminar consisting of talks and presentations of ACOA experts. In addition, about 50 people participated online. The seminar was held at Code Academy, a company member of ACOA
https://akta.az/news/cybersecurity-trends-adli-seminarimiz-ugurla-kecirilib

Organized the first networking event of ACOA experts
https://akta.az/news/akta-ekspertlerinin -ilk-sebekelesme-tedbiri-kecirildi

Conduct a seminar at the Azerbaijan Technical University (**AzTU**) within the framework of the Cyber Security Awareness Month. The seminar jointly

organized by ACOA and AzTU provided the students about cyber war and dark web. More than 300 students from the university participated in the seminar *https://akta.az/news/azerbaycan-texniki-universitetinin-telebeleri-uecuen-kibertehluekesizlik-moevzusunda-seminar-kecirilib*

1st Conference on Cyber Hygiene - Safe Digital Environment

Azerbaijan State Pedagogical University (**ADPU**) and ACOA jointly organized an educational event on trends in the field of cybersecurity and the importance of integrating cybersecurity education into schools. ADPU told Azerbaijan State News Agency (**AZERTAC**) that Rector Jafar Jafarov gave information about the university and emphasized the special importance of cybersecurity in the 4th Industrial Revolution *https://akta.az/news/kibertehluekesizlik-tehsili-ile-bagli-maariflendirme-aparilib*

19 Dec 2023 - an event reporting the activities of ACOA for 2023. Leaders and representatives of legal entities that are members of ACOA General Meeting, as well as ACOA partner institutions and organizations, including higher education institutions and companies, participated in the reporting event *https://akta.az/news/azerbaycan-kibertehluekesizlik-teskilatlari-assosiasiyasinin-akta-2023-cue-il-uezre-fealiyyetine-dair-hesabat-tedbiri-kecirilib*

22 Dec 2023 - a round table meeting on the topic '*Cybersecurity in the financial markets sector*' under the joint organization of ACOA and the Azerbaijan Banks Association (**ABA**) *https://akta.az/news/maliyye-bazarlari-sektorunda-kibertehluekesizlik-moevzusu-uezre-deyirmi-masa-formatinda-muezakire-kecirilib*

1.3.2 Event Involvement

ACOA participated in the CyberTech Global Tel-Aviv conference during a business trip to Israel. Active discussions and exchange of ideas on current topics of cyber security *https://akta.az/news/akta-heyeti-beynelxalq-sergide-istirak-edir*

ART2023 robotics tournament organized by Azerobot company, a member of the Management Board of ACOA with the support of ACOA *https://akta.az/news/akta-idare-heyetinin-uezvue-azerobot-sirketinin-teskilatciligi-ve-akta-nin-desteyi-ile-art2023-robototexnika-turniri-bas-tutmusdur*

ACOA met with Israel State CERT discussing the characteristics of the cybersecurity ecosystem of the countries, future cooperation, and other issues *https://akta.az/news/azerbaycan-kibertehluekesizlik-teskilatlari-assosiasiyasi-akta-israil-doevlet-cert-i-ile-goeruesdue*

The cybersecurity training organized within the framework of the project Education on Cybersecurity in General Educational Institutions funded by the Ministry of Science and Education of the Republic of Azerbaijan and implemented by ACOA. Coordinators of Barda, Ganja, Shirvan, and Lankaran STEAM centres were presented with relevant certificates for the training *https://akta.az/news/uemumi-tehsil-mueessiselerinde-kibertehluekesizlik-uezre-maariflendirmenin-aparilmasi-layihesi-cercivesinde-teskil-olunmus-kibertehluekesizlik-telimleri-basa-catib*

With the financial support of the Youth Fund of the Republic of Azerbaijan, ACOA, and the technical support of the AzeRobot Education Educational Center, the project of the European Student Forum-Sumgayit Public Union Acquisition of ICT Knowledge of Young Girls and Digital Transformation of the Economy was finalized. The events took place in Koroglu, Mashtağa, Balakhani branches of AzeRobot Education Robotics Training Center *https://akta.az/news/akta-xanimlarin-ikt-bacariqlarinin-inkisafina-destek-verir*

13 April 2023 , – Organized a in telebridge format business conference to develop IT experience and business relations between Azerbaijan and Russia. The events were held in Baku and Moscow and attended by company heads, state representatives, and business associations from both sides *https://akta.az/news/akta-moskva-baki-it-sahesinde-emekdasliq-konfransinda-istirak-edib*

11 May 2023 - the 1st International Conference dedicated to the 4th Industrial Revolution and IT started at Azerbaijan State Oil and Industry University. ACOA was among the organizations participating in the conference. ACOA's Deputy Chairman Rauf Jabarov spoke at the opening of the conference about the importance of scientific works and research projects in the field of cybersecurity *https://akta.az/news/akta-beynelxalq-konfransda-istirak-edib*

18 Jun to 1 Jul 2023, South Korea - Elvin Balajanov, Chairman of the Board of ACOA, participated in the Cyber Security Capacity Building (Azerbaijan) ('21-'23)' project implemented by the Korea International Cooperation Agency (**KOICA**) to strengthen the personnel potential in cybersecurity. He was on a business trip *https://akta.az/news/akta-idare-heyetinin-sedri-18-iyun-01-iyul-tarixlerinde-cenubi-koreya-respublikasinda-isguezar-seferde-olub*

13 Sep 2023 Almaty, Kazakhstan - Elvin Balajanov, chairman of ACOA Board of Directors, participated in the KazHackStan 2023 - Turan 2023 Conference and attended by more than 3,000 local and foreign experts and visitors *https://akta.az/news/regionda-kibertehluekesizliyin-daha-effektiv-ve-semereli-temin-olunmasi-tuerk-doevletleri-teskilatina-uezv-oelkeler-arasinda-emekdasligin-genislendirilmesini-sertlendirir*

3 – 4 Oct 2023 - ACOA participated in the Central Eurasian Cyber Security

Summit held in the Republic of Uzbekistan *https://akta.az/news/akta-3-4-oktyabr-2023-cue-il-tarixlerinde-oezbekistan-respublikasinda-kecirilen-merkezi-avrasiya-kibertehluekesizlik-sammitinde-istirak-edib*

26-27 Oct 2023 – Critical Infrastructure Defense Challenge 2023 jointly organized by the State Service for Special Communication and Information Security of the Republic of Azerbaijan (**XRITDX**) and the State Security Service of the Republic of Azerbaijan and the partnership of at the Baku Congress Center. A two-day event called CIDC-2023) was held *https://akta.az/news/critical-infrastructure-defense-challenge-2023-cidc-2023-adli-tedbir-kecirildi*

A visit by Babes-Bolyai University, located in the city of Cluj, which is considered the Silicon Valley of Romania. At the meetings, ACOC Board Chairman Elvin Balajanov talked about the educational and research activities carried out by the higher educational institutions of the Republic of Azerbaijan in the field of information security and cyber security, as well as the projects implemented by the Association, the works carried out to strengthen the relations between educational institutions and industry

Later, a meeting was held with Azerbaijani students studying at Babesh-Bolyai University discussing the students' thoughts and experiences about their studies, the study and research environment, as well as opportunities available for them at ACOA *https://akta.az/news/ruminiyanin-silikon-vadisi-hesab-edilen-kluj-seherinde-yerlesen-babes-bolyai-universitetine-sefer-edilib*

1.3.3 Achievements

15 April 2023 – Signing of the Memorandum of Cooperation between ACOA and the Baku Higher Oil School. This is on the implementation of joint projects and research and on effective information exchange to promote the organization of the exchange and to define the common areas in which the cooperation will be carried out. The aim is strengthening the ecosystem in the field of cybersecurity, including the establishment of public and business relations *https://akta.az/news/azerbaycan-kibertehluekesizlik-teskilatlari-assosiasiyasi-ve-baki-ali-neft-mektebi-arasinda-emekdasliq-memorandum-imzalanib*

ACOA was selected as a member of the OIC-CERT cooperation platform *https://akta.az/news/akta-oic-cert-emekdasliq-platformasina-uezv-secilib*

1.3.4 Events Organized by ACOA

CTF competition dedicated to the International Cyber Security Day

The 1st Conference on Cyber Hygiene called '*Safe Digital Environment*'

1st Conference on cyber hygiene 'Safe Digital Environment'

The 1st Summit of CISOs of the state institutions dedicated to *Safer Internet Day*

1.3.5 Events Involvement

Fintex Summit Finance and Technology Conference

Fintex Simmit

International Cyber Security Days Conference held by the PROSOL company

Global Hybrid War and Cyber Security Summit co-organized by InterProbe and ACOA

Global Hybrid Warfare & Cybersecurity Summit

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

Istanbul, Turkey - Regional Cybercrime Cooperation Exercise funded by EU Cybersecurity East project

Baku, Azerbaijan - National Workshop on cybercrime reporting, use of cyber taxonomies and coordinated Internet Organised Crime Threat Assessment (**iOCTA**) reporting organised under the EU Cybersecurity East project

Muscat, Oman - OIC-CERT 10th General Meeting & 14th Annual Conference

OIC-CERT 14 Annual Conference

Energy Crisis and Cybersecurity event at Azerbaijan State Oil and Industry University

Energy Crisis & Cybersecurity

1.4 ACHIEVEMENTS

Recorded and handled 480.4 million incidents by NGFW, 3.7 million malware by centralized endpoint security system and 223 000 malicious documents with the special sandbox

Prevented specifically targeted APT cyberattacks by identifying and blocking 1,192 IOCs

Blocked 48 impersonated state domains detected by various TI tools

The largest observed DDoS attack lasted for 8 days (137Gb and 19 million rps.) and ensured uninterrupted activity of the state websites

Processed a total of 27.8 million e-mails through the State E-mail Service and blocked 2.2 million due to 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 the necessary security measures

Prepared and implement *Information Security Policy* to the 90 state institutions

Started the cyber hygiene project with 130 state institutions participating involving 4474 employees where 3990 of them were involved with the online training

EU Conference

Implemented the Azerbaijani language to the SIM3 Self-Assessment tool

Published the Information Security Journal for free for government bodies

Participate in several TV programs to raise awareness

Discovered high-risk zero-day vulnerability in the global e-mail service by Ice Warp Inc. (CVE-2022-35115)

Published and distributed 5,000 desktop calendars to state institutions for the purpose of awareness as part of the Information Security Calendar project plan

1.5 PLAN FOR 2024

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 transferred data and keep them within the country boarders

Continue collaboration with CERTs internationally

Information Security Journal published in 2023

2 BANGLADESH

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

2.1 ABOUT THE ORGANIZATION

2.1.1 Introduction

The Bangladesh Government's Computer Incident Response Team (**BGD e-GOV CIRT**) is acting as the National CERT of Bangladesh (**N-CERT**) responsible for 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 with broad cybersecurity ramifications, conducts research and development, and provides guidance on security vulnerabilities

BGD e-GOV CIRT collaborates with various government units, CII, financial organizations, law enforcement agencies, academia, and civil society to help improve the cybersecurity defence of Bangladesh

2.1.2 Establishment

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

2.1.3 Resources

Currently there are 17 people working in BGD e-GOV CIRT

2.1.4 Constituency

Constituencies of BGD e-GOV CIRT are all governmental, semi-governmental, autonomous bodies, ministries, and institutions of Bangladesh. Currently BGD e-GOV CIRT is acting as the National CERT of Bangladesh with a mandate to serve the whole country

2.2 HIGHLIGHTS OF 2023

2.2.1 Summary of Major Activities

BGD e-GOV CIRT has successfully organized the Financial Institution & CII Cyber Drill 2023

BGD e-GOV CIRT has successfully organized the Cyber-Maitree 2023 and

cybersecurity training & exercise in association with CERT-In

Financial Institution & Critical Information Infrastructure (CII) Cyber Drill 2023

Cyber-Maitree 2023, Cybersecurity training and exercise

A total of 98 meticulously crafted cyber threat alert reports were distributed to diverse organizations across Bangladesh

Responding to three major ransomware incidents reported to BGD e-GOV CIRT throughout the year.

Cyber Threat Intelligence Report provided to 71 government and non-government organizations

Twelve (12) cyber sensor analysis reports have been provided to multiple CII

Vulnerability assessment and penetration testing (**VAPT**) have been performed on different sectors in Bangladesh including the financial sectors, CII, and Govt. sectors

2.3 ACHIEVEMENTS

Published 'Ransomware Landscape: A Data-driven Threat Analysis of Bangladesh, Year 2023'

Abu Dhabi, United Arab Emirates - Participated in the 11th Regional Arab, OIC-CERT, and CIS Cyber Drill

Participated in the APCERT Cyber Drill 2023 '*Digital Supply Chain Redemption*'

2.4 ACTIVITIES & OPERATIONS

2.4.1 Events organized by BGD e-GOV CIRT

BGD e-GOV CIRT has successfully organized the Financial Institution & CII Cyber Drill 2023

BGD e-GOV CIRT has successfully organized Cyber-Maitree 2023 and cybersecurity training & exercise in association with CERT-In

Organized a 5-day training session for officials of the Palli Karma-Sahayak Foundation (**PKSF**)

Organized training for officials of ICT division on cybersecurity awareness and social engineering aspects

5 days long training session for officials of PKSF

Organized MIST LeetCon 2023, '*Hack Me If You Can*'

Organized Safe CII Workshops for all the CII organizations of Bangladesh

Supported partner in cybersecurity conference RenasCON 2023

Organized a one-day seminar, titled '*Secure Our World*', at the event of Cyber Security Awareness Month 2023 for women entrepreneurs

2.4.2 Events involvement

Participated in Cyber Defence Conference 2023

Conducted training session at the Armed Police Battalion (**APBn**) Headquarters

Training session at APBn

Conducted a session on capacity building on cybersecurity for RAJUK Officials

USA - Attended the RSA Conference 2023

Capacity Building on Cybersecurity for RAJUK

Conducted training session at the Cyber Training Centre, Criminal Investigation Department (**CID**)

Singapore - Attended the *Black Hat Asia 2023*

Cyber Training Centre, CID

Conducted training on CIRT operation and digital forensics at the Office of the Controller of Certifying Authorities (**CCA**)

Participated in the Cyber Championship, organized by the National Cyber Range of Russia

Conducted a 5-day training session for officials of the Department of ICT in cooperation with the *Enhancing Digital Government & Economy* (**EDGE**) project

Conducted a one-day training session on Cybersecurity Challenges in 4IR Revolution at the Security Services Division under the Ministry of Home Affairs of Bangladesh

USA - Participated in the '*Financial Sector Tech Camp #1*' conducted by

Carnegie Mellon University, organized by the State Department

Conducted a 5-day training session for officials of the CII organizations, organized by EDGE project

"Case study on Spear Phishing" at System Administrator's Day 2023, organized by BDSAF

Conducted a session on Case Study on Spear Phishing during the System Administrator's Day 2023, organized by Bangladesh System Administrators Forum (**BDSAF**)

Cybersecurity training for CII

Conducted a 2-day training session on cybersecurity awareness for Female Member of the Parliament, organized by the EDGE project

Conducted a 2-day training session on Cyber Security Act 2023, digital forensics, and social engineering for the officials of Corps of Military Police Center and School

Conducted training on cybersecurity for officials of Police Telecom and Information Management, Bangladesh Police

Two days training session on Cybersecurity Awareness for Female Member of Parliament

Conducted training session on cybersecurity awareness and *Cyber Security Act 2023* at the Department of Women Affairs

Participated in the Cyber Security Symposium 2023 organized by Bangladesh System Administrators Forum on the event of Cyber Security Awareness Month 2023

Participated in discussion on Cyber Security Awareness Month 2023 at Dutch-Bangla Bank Ltd. along with all the department heads and branch managers around the country

Participated in Cyber Security Conference 2023, titled '*Flag Hunt Take0ver*', at Military Institute of Science and Technology (**MIST**), powered by IT Directorate, Bangladesh Army

Participated in a seminar on Smart Bangladesh and Cybersecurity organized by Smart Bangladesh Network and Innovation Design and Entrepreneurship Academy (**IDEA**)

Participated in a round table meeting on Risks and Opportunities for Youth and Young Women in Information Technology organized by the daily newspaper Samakal

Risks and opportunities for youth and young women in information technology

Abu Dhabi, United Arab Emirates - Participated the following events in the Regional Cybersecurity Week 2023

- The 11th Regional Arab, OIC-CERT & CIS Cyber Drill
- The 11th Regional Cybersecurity Summit
- The 15th Annual OIC-CERT Conference and Forum for Incident Response Team (**FIRST**) Symposium for Arab and Africa Regions

2.4.3 Achievements

Provided twelve (12) Cyber Sensor Analysis Report (Jan - Dec 2023) to multiple CII

Cyber Threat Intelligence Report provided to 71 government and non-government organizations

Published cybersecurity magazine for stakeholders

Performed risk-based audit for CIIs and government organizations

Digital forensics service provided to seven (7) organizations. Eight (8) cases where 28 artifacts were analysed

A total of 98 meticulously crafted cyber threat alert reports were distributed to diverse organizations across Bangladesh. These reports aimed to fortify the preparedness and resilience of stakeholders against emerging cyber threats

Additionally, the CTI unit proactively enhanced cyber awareness and readiness within the national landscape by authoring and disseminating 10 comprehensive cybersecurity advisories and awareness materials. These initiatives were instrumental in empowering stakeholders and the public with the knowledge and best practices necessary to effectively mitigate cyber risks

The CTI team played a pivotal role in responding to three major ransomware incidents reported to BGD e-GOV CIRT throughout the year

To deepen the understanding of the ransomware threat landscape specific to Bangladesh, the CTI division published '*Ransomware Landscape: A Data-driven Threat Analysis of Bangladesh, Year 2023*.' This insightful analysis provided stakeholders with valuable insights derived from empirical data, enabling informed decision-making and the formulation of robust cyber defence strategy

2.5 2024 PLANNED ACTIVITIES

Arrange Cyber Drills for different sectors

Perform risk-based audit for CIIs and Government organizations

Provide training about Industrial Control System (**ICS**) in the Public sector

Perform vulnerability assessment and penetration testing on financial sectors

Training and workshop about cybersecurity for government organizations

Provide regular cyber sensor analysis report such as intrusion and suspicious activities to CII where the cyber sensors are deployed

"Safe CII" workshop for CII organizations

Cybersecurity training for Government officers

Attended "RSA Conference 2023", USA

Attended "Black Hat Asia 2023, Singapore

Participated in Cyber Défense Conference 2023

Supported partner in Cyber Security conference renasCON 2023

3 BRUNEI DARUSSALAM

Brunei Computer Emergency Response Team - BruCERT

3.1 ABOUT THE ORGANIZATION

3.1.1 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 cyber security threats and cyber-crime. It operates under the Ministry of Transport and Infocommunications (**MTIC**), with the Minister of MTIC as Minister-in-charge of Cybersecurity

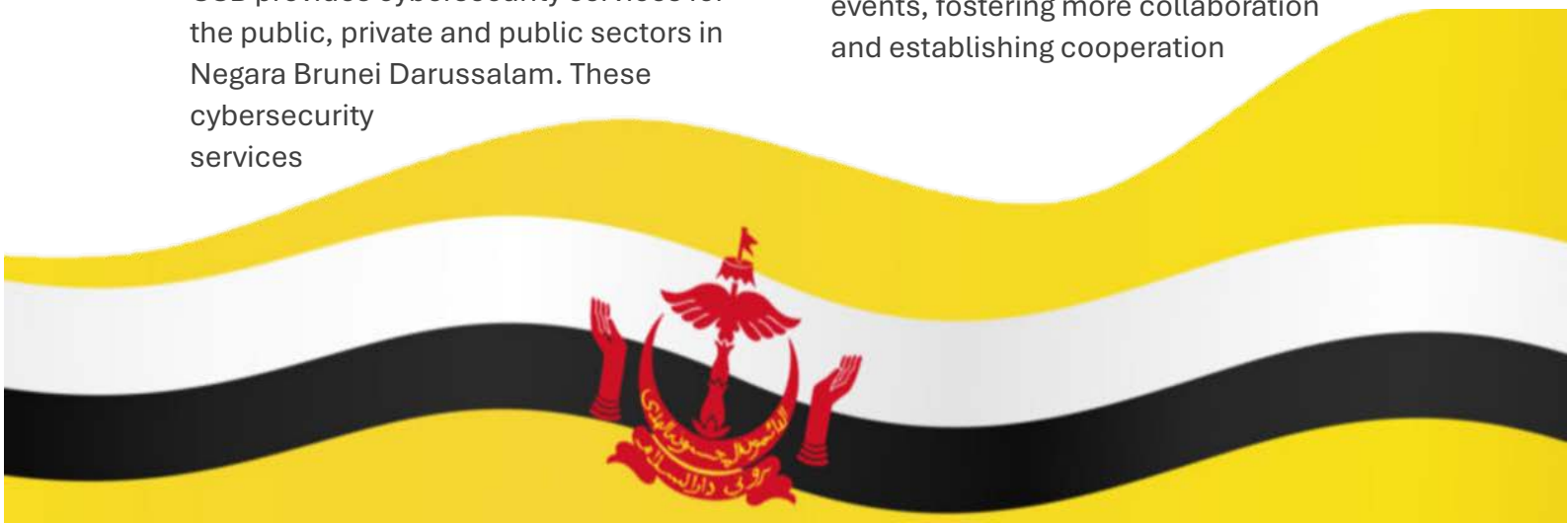
CSB provides cybersecurity services for the public, private and public sectors in Negara Brunei Darussalam. These cybersecurity services are intended to ensure the following interests:

- Increase awareness of cyber threats in the public and private sectors, especially in the protection of 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 on cyber threats

BruCERT was established in May 2004. It was formed in collaboration with Authority for Info-communications Technology Industry of Brunei Darussalam (**AITI**) and the Ministry of Communication, to become the nation's first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents in Brunei Darussalam. It is now under Cyber Security Brunei

BruCERT join the Asia Pacific Computer Emergency Response Team (**APCERT**) in 2005, OIC-CERT in 2009 and FIRST in 2014

BruCERT has been actively participating in the local as well as international events, fostering more collaboration and establishing cooperation



with other relevant organisations and CERT's

- BruCERT Services

24X7 security related Incidents and emergency response from BruCERT

24X7 security related incidents and emergency response onsite (deployment of responses is within 2hrs after an incident report is received). This service only applies to BruCERT Constituents

Broadcast alerts/ early warnings on new vulnerabilities, advisories, viruses and security guidelines at BruCERT website. BruCERT Constituents will receive alerts through email and telephone as well as defence strategies in tackling IT security related issues

Promote Security Awareness program to educate and increase public awareness and understanding of information security and technical know-how through education, workshop, seminar, and training

Coordinating with other CERT, network service providers, security vendors, government agencies as well as other related organizations to facilitate the detection, analysis, and prevention of security incidents on the Internet

3.1.2 BruCERT Establishment

BruCERT coordinates with the local and international Computer Security Incident Response Team (**CSIRT**s), network service providers, security vendors, law enforcement agencies (**LEA**s) as well as other related organizations to facilitate the detection, analysis, and prevention of security incidents on the Internet

3.1.3 BruCERT Workforce

BruCERT currently has a strength of 66 staff (100% local) of which majority specializes in IT, while the rest are 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 BruCERT workforce has gained certifications in

3.1.4 BruCERT Constituents

BruCERT has close relationships with the government agencies, 1 major ISP, and various numbers of vendors

- Government Ministries and Departments

BruCERT provide security incident response, managed security services via Cyber Watch Centre (**CWC**) and Consultancy services to the government agencies. Security trainings such as forensic and awareness trainings were provided by BruCERT in collaboration with some government agencies

- E-Government National Centre

The E-Government National Centre (**EGNC**) provides IT services to all government departments and ministries in Brunei Darussalam. Services such as IT Central Procurement, Network Central Procurement, Co-location,

ONEPASS (a PKI initiative), 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 resided at EGNC

- AITI

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

- The Royal Brunei Police Force and Law-Enforcement Agencies

BruCERT has been collaborating with Royal Brunei Police Force (**RBPF**) and other LEAs to resolve computer-related incidents through BruCERT's Digital and Mobile Forensic services

- Unified National Network

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

- Brunei Cyber Security Association

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

3.1.5 BruCERT Contact

BruCERT Coordination Centre welcome reports on computer security related incident. Any computer related security incident can be reported to:

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

3.2 BRUCERT OPERATION 2023

3.2.1 Incidents response

For 2023, CSB's BruCERT through the 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 especially those involving Ransomware. The second most common type of incident detected involved attacks on user accounts, including both normal user and privilege accounts. The following diagram depict the statistics of these security incidents

Denial Of Service
0% was detected within the monitored network

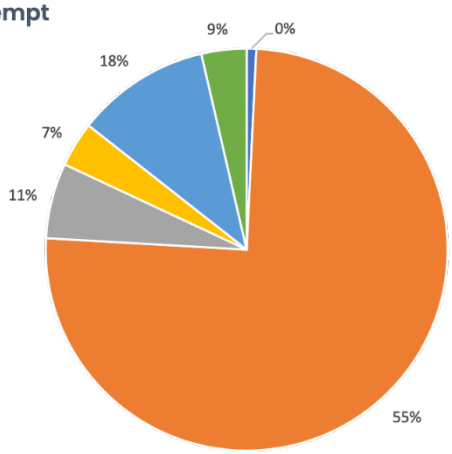
Unsuccessful Hacking Attempt
7% was detected within the monitored network

Malware
55% was detected. within the monitored network

Privilege User account
11% was detected within the monitored network

Reconnaissance
11% was detected within the monitored network

Normal User Account
9% was detected within the monitored network

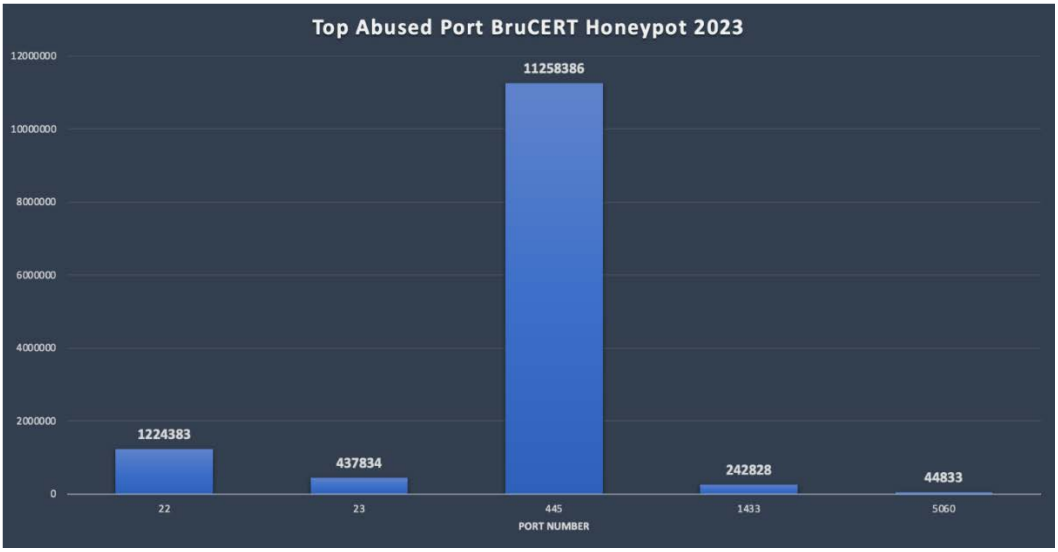


TYPE OF ATTACK	COUNT
Denial of Services	4
Malicious Software	1746
Reconnaissance	345
Unsuccessful Hacking Attempt	221
Normal User Account	300
Privilege User Account	555

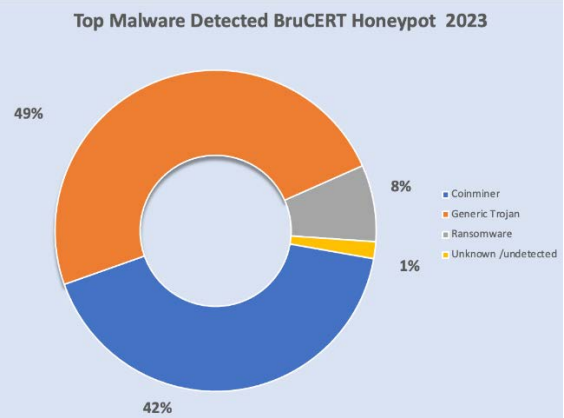
Malware outbreak within BruCERT constituents had decreased from 2022 due to successful deployment of CSB's End point Detection Response (**EDR**) system. The deployment of EDR CWC had detected an increased amount of reconnaissance upon the constituents which were suspected perform by malicious software

3.2.2 BruCERT Honey Pot

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



PORT NO	COUNT
22	1224383
23	437834
445	11258386
1433	242828
5060	44833

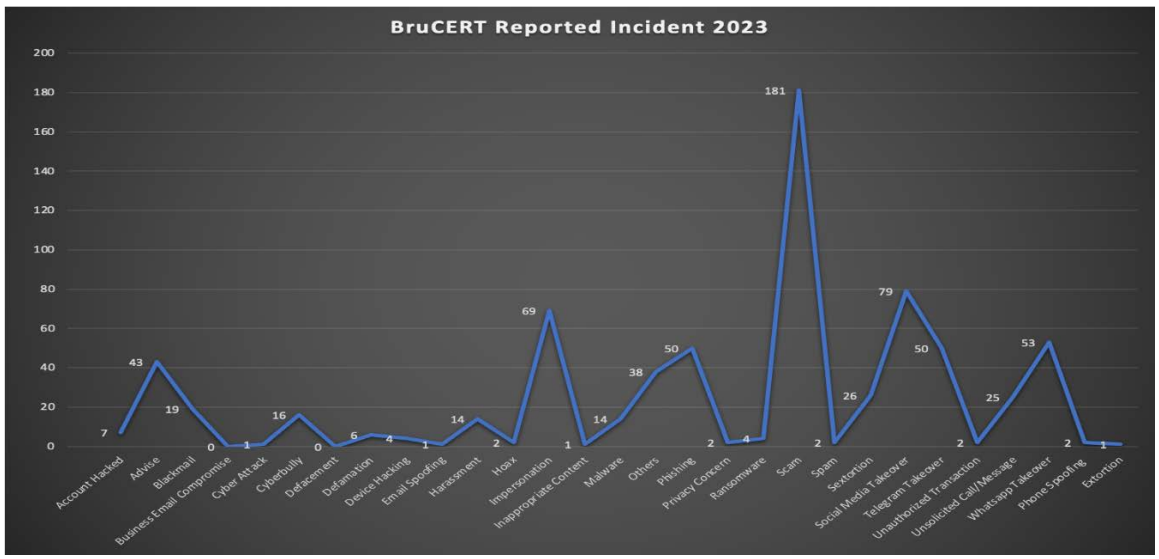


From the BruCERT honey pot, it seems new variants of malware had been targeting the organizations using port 22 as well as port 445. This can be further analysed from the malware which was captured by BruCERT honeypot shown by the following diagram. In other configuration, BruCERT Honeypot managed to capture some of the malware hashes. The following diagram and table show the summary of the most detected malware attacking the Honeypot

MALWARE TYPE	TOTAL
COINMINER	7081
GENERIC TROJAN	8261
UNKNOWN	287
TOTAL	16936

In 2023, BruCERT has been receiving incident reports from the public and the private sector. Most of these reports pertained to Scam activities followed by Social Media Issues. The former included instances of social media accounts such as Instagram, Facebook, WhatsApp, and Telegram being successfully compromised or taken over, with an increase in such incidents observed in Brunei Darussalam

Compromised social media accounts were often used as part of the scam activities. There has been a rise in scam activities for the past three years targeting Bruneians, utilizing local Brunei language and culture as shown in the following diagram



3.3 BRUCERT ACTIVITIES 2023

3.3.1 Seminars/ Conferences/ Meetings/ Visits

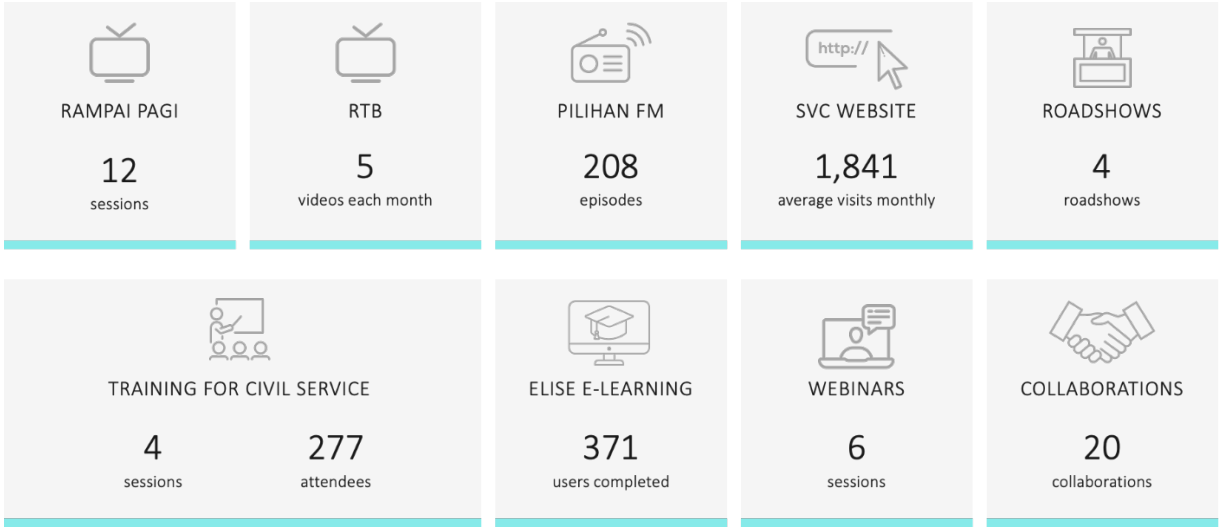
BruCERT attended and presented at various seminars, conferences, and meetings related to the field of ICT security and some of the meetings are done online

8 - 9 Nov 2023 Online - BruCERT delegates attended the online APCERT Annual General Meeting and Annual Conference 2023

16 – 20 Oct 2023 Abu Dhabi, UAE - Three BruCERT staffs attended the OIC-CERT 15th Annual Conference hosted by the UAE Cyber Security Council

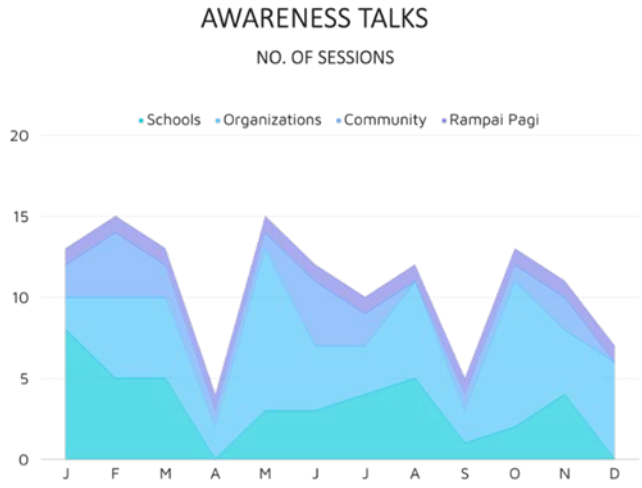
3.3.2 Awareness Activities

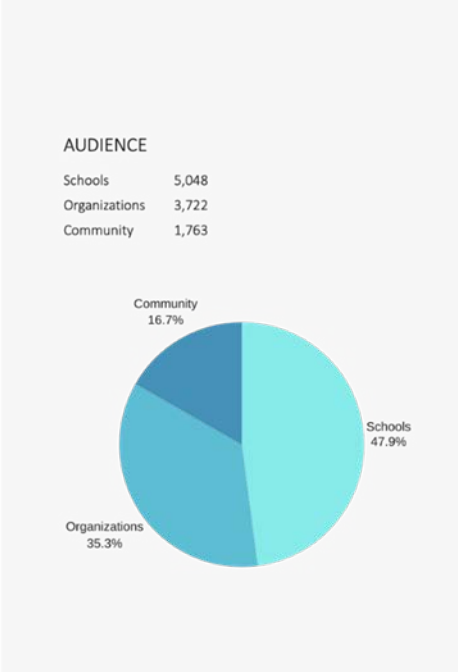
Throughout 2023, CSB via BruCERT conducted various awareness-raising activities aimed at educating both the public and government staffs about the security threats present in the cyber world. BruCERT awareness website for this program is *www.secureverify connect .info*, which received an average of 1,841 monthly website visits. The following diagram shows the BruCERT Awareness infographic activity for the year 2023



'*Rampai Pagi*' is a live local interview segment on Friday morning where awareness personnel from BruCERT interviewed and provide insights on various security topics throughout 2023

BruCERT awareness talk which was provided to schools, community as well as corporate/ organization also took place almost every month in the year 2023. A total number of 5,048 students, 3,722 personnels from various organizations, and 1,763 elderly had attended BruCERT awareness talk in 2023


AWARENESS TALKS
NO. OF SESSIONS
Schools
Organizations
Community
Rampai Pagi
20
15
10
5
0
J
F
M
A
M
J
J
A
S
O
N
D


AUDIENCE
Schools 5,048
Organizations 3,722
Community 1,763
Community
16.7%
Schools
47.9%
Organizations
35.3%


@mtcitoman
سلطنة عُمان
وزارة النقل والاتصالات وتقنية المعلومات
Sultanate of Oman
Ministry of Transport, Communications and
Information Technology

4 INDONESIA

National Cyber & Crypto Agency - NCCA

4.1 ABOUT THE ORGANIZATION

4.1.1 Introduction

The government agency which has a national responsibility in cybersecurity started with the establishment of 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 works under the Directorate of Telecommunication of the Ministry of Communication and Information. Based on the Presidential Decree Number 53 in 2017, Id-SIRTII/ CC merged and moved to 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

4.1.2 Establishment

Id-SIRTII/ CC was established on 4 May 2007 and later merged with the National Crypto Agency to become NCCA, based on the Presidential Decree Number 53 in 2017. NCCA officially started its operation in Apr 2018

4.1.3 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 government, CII, and digital economy sector

4.1.4 Constituency

- Ministries and Government agencies
- LEAs

- National Defence
- CII Operators
- Cybersecurity communities
- Internet Service Providers (ISP)
- Network Access Providers (NAP)
- Local Internet Exchange Operators
- Other sector CERT/ CSIRT in Indonesia

4.2 HIGHLIGHTS OF 2023

4.2.1 Summary of Major Activities

2023 marked a more progressive year compared to previous years, especially following the recovery from the Covid-19 pandemic. NCCA was more actively involved in various national and international events, including cybersecurity task forces, capacity building, cyber drills, and others. Regulation-wise, NCCA also succeeded in issuing several regulations that promote the enhancement of national critical infrastructure security in Indonesia, as well as maturing the CSIRT ecosystem in Indonesia which continues to grow

National CSIRT Annual Forum

4.2.2 Achievements

2023 was a highly progressive year for the Na CCA in carrying out the mandate of Indonesian President Joko Widodo who issued Presidential Decree No. 82 of 2022 on the Protection of Vital Information Infrastructure. During this time, the NCCA successfully released regulations concerning Identification on Vital Information Infrastructure, Vital Information Infrastructure Framework, Cybersecurity Maturity Measurement, as well as the publication on Regulation of the President of the Republic of Indonesia Number 47 of 2023 on National Cyber Security Strategy and Cyber Crisis Management. These regulations serve as references for NCCA in implementing efforts for national cybersecurity protection and making significant contributions to the international scope

4.3 ACTIVITIES & OPERATIONS

4.3.1 Events organized by NCCA

As the Deputy Chair of OIC-CERT, Indonesia also holds the responsibility to implement the 5th pillar of OIC-CERT: business plan which is Capacity Building. In 2023, NCCA organized several events to enhance the knowledge and capabilities of the OIC-CERT member countries as follows

31 Mac 2023 – Technical Workshop '*The Role of ISACs in Improving Cybersecurity and Resilience: Introduction and Implementation of Best Practice*'

3 Aug 2023 – 'ISACs Introduction and Implementation Best Practice for Management Level: Building And Managing Isac in Government Sector'

16 Oct 2023 - ISACs Vulnerabilities Webinar in collaboration with Huawei Indonesia

- 27 Nov 2023 – Workshop on *'Data Protection in Cybersecurity - A Critical Imperative'*

As the National CSIRT, IDSIRTII/ CC under NCCA also organized a National CSIRT Annual Forum to gather CSIRTs from different sectors in Indonesia, conducted exhibitions at the National Cybersecurity Contest, and played a role in the INDOSEC Summit 2023 event. Internationally, collaborating with Korea Internet Security Agency (**KISA**) for Cybersecurity Joint Program, NCCA held the Seminar & Hands-on Exercise - Global Cybersecurity Center for Development (**GCCD**), which focused on digital forensics

4.3.2 Events involvement

NCCA also participated and was involved in many international events among them are as follows

F5 API Hackathon by F5

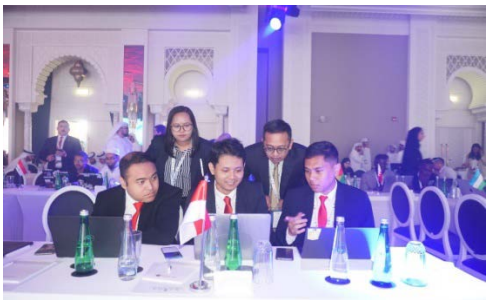
The United Nations Office on Drugs and Crime (**UNODC**) Trainings and Workshops on Cyber Crimes

Civilian Research and Development Foundation Global (**CRDF GLOBAL**) Threat Space Workshop: '*Cyber Capacity Building for Highly Trafficked Ports'* in collaboration with Mandiant

UAE CSC and EXPO2020 Dubai – *Cyber Protective Shield Global Cyber Exercise*

OIC-CERT Annual Meeting and ARCC Regional Cyber Drill

Microsoft Cybersecurity and Personal Data Protection Roundtable



OIC-CERT Annual Conference & Drill

International Law Enforcement Academy (**ILEA**) DarkWeb Investigation and Cryptocurrency Investigative

Regulatory Training Course on Cryptocurrencies *Supervisory Best Practises Workshop*

ASEAN Japan Cybersecurity Capacity Building Centre (**AJCCBC**) Cybersecurity Technical Training

The Asia Pacific Internet Security Conference Security Training Course (South Korea)

Asia Pacific Internet Security Conference Training Course

- ASEAN Cyber Shield Hacking Contest
  - ILEA Investigating Criminal Use of Cryptocurrency Training
  - Workshop by Cybersecurity & Infrastructure Security Agency (**CISA**), USA
  - Human Resource Development for Cyber Security Professionals

(Bhutan GoVTech Agency visits to IDSIRTII), etc

ILEA DarkWeb Investigation and Cryptocurrency Investigative

4.4 ACHIEVEMENTS

As the National CSIRT, NCCA has aided 83 cybersecurity incident cases and delivered 55 digital forensics services in 2023, primarily to government sector organizations

2023 also marked a significant milestone for the agency, with the certification of the Digital Forensic Laboratory with ISO/IEC 17025:2017 Accreditation Certificate. NCCA successfully deployed honeypots in the Honeynet program at 105 points spread across 27 provinces in Indonesia. NCCA also continues to strengthen cybersecurity in Indonesia by encouraging organizations in critical sectors to establish their own CSIRT. Throughout 2023, a total of 136 new CSIRTs were formed, expanding the CSIRT ecosystem in Indonesia to 306 teams by the end of 2023

Certification of the Digital Forensic Laboratory with ISO/IEC 17025:2017

NCCA has also published the Indonesia Cybersecurity Landscape Report 2023 that can be accessed through this link: *https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html*

4.5 2024 PLANNED ACTIVITIES

Based on the results of the 2022 OIC-CERT Board Election, Indonesia once again holds the role as Deputy Chair of OIC-CERT till 2024. We still hold the role of carrying out the Capacity Building pillar, so the agency plan to hold several more training activities in the form of webinars and workshops. However, in the OIC-CERT AGM, Indonesia will still propose to contribute primary role as a board member

At the national scale, Indonesia will hold several international events, involved in many cybersecurity task forces in national events, and will continue to support the establishment of a bigger CSIRTs ecosystem

5 JORDAN

National Cyber Security Center - NCSC

المركز الوطني للأمن السيبراني
National Cyber Security Center

5.1 ABOUT THE ORGANIZATION

5.1.1 Introduction

NCSC is a governmental institution that aims to build, develop, and manage an effective cybersecurity system at the national level. This involve protecting the Kingdom from cyberspace threats and confront them efficiently and effectively in a way that ensures the sustainability of work and maintains national security and the safety of people, property, and information. In creating a safe and reliable Jordanian cyberspace, NCSC seeks to train, qualify, raise awareness, and educate the public and private sectors' employees and all segments of the society, and provide them with the knowledge and skills necessary to reduce the level of risks and threats according to best practices in the field of cybersecurity in a way that ensures the highest level of efficiency, and to make Jordan a centre of regional and international creativity and excellence in this field

5.1.2 Establishment

NCSC was established in accordance with Article No.(5/A) of the Cybersecurity Law No. (16) of 2019, as a specialized institution responsible for everything related to national cybersecurity. NCSC has a legal personality with financial and administrative independence and is affiliated with the prime minister and entrusted with the tasks of building an

effective cybersecurity system at the national level. In addition to developing and organizing cybersecurity requirements to protect the Kingdom from cyber threats and mitigate them efficiently and competently, the agency need to ensure the sustainability of work and preserve national security and the safety of people, property, and information

5.1.3 Resources

General budget allocates financial resources to fund NCSC annually

5.1.4 Constituency

National level: public and private sectors

5.2 HIGHLIGHTS OF 2023

5.2.1 Summary of Major Activities

Expansion of Security Information and Event Management (**SIEM**) in the centre

Equipping the Government Security Operation Centre (**SOC**) in the centre

Equipping the data centre room in the centre

Launching the cyber information sharing platform – SHARE

Launching Continuous penetration - Bug Bounty

Launching Jordan CERT (**JOCERT**) National Cybersecurity Incident Response Team website

Launching *Safe Online* platform

Joining the public administration modernization roadmap and economic modernization vision in the Kingdom

Presenting a draft of the National Cybersecurity Framework for public consultation

Joining the FIRST forum

Joining Trusted Introducer CSIRT (**TI-CSIRT**)

Joining the OIC- CERT

Joining ITU – Arab Regional Cybersecurity Center (**ARCC**)

Strengthening the capabilities and enhancing the skills of employees and workers in the national sectors

5.3 ACHIEVEMENTS

Holding the first National Cybersecurity Summit "*Dot Cyber Summit 2023*"

Signing a total of twelve (12) MoU with the academic, private, and public sectors and 2 MoU with international and regional parties

Publishing cybersecurity products accreditation policy for the ministries and government institutions

Publishing cybersecurity incidents classification instructions

5.4 ACTIVITIES & OPERATIONS

5.4.1 Events organized by the organization/ agency

Cyber Nashama Camp aims to develop the skills of university graduates in IT majors from all Jordanian universities in the practical fields of cybersecurity

Cyber Warriors Competition aims to provide technical challenges on many cybersecurity topics such as vulnerabilities, hacking, reverse engineering, and others, which is known as CTF

CTF Training which is a training program dedicated to students of all public and private universities to train them on the challenges of CTF

Cyber Pioneers which is dedicated to students at Jordanian schools with the aim of developing awareness among students and teaching them about the dangers of using the Internet and consequences

Dot Cyber Summit 2023 which covered both public and private sectors challenges in the cybersecurity field, and brought together experts and professional in the field who provided insights and practical solutions to overcome the wide-ranging security and best practices

5.4.2 Events involvement

Attended/ participated in the following

Open-ended Working Group (**WG**) on security in the use of ICT 2021–2025

France, Convergence 2023

Netherlands, Cisco Live,

Arab Experts Group on Combating Information Technology Crimes, 3rd meeting

Qatar, The National Cyber Drill

Bahrain, The Arab International Cybersecurity Exhibition and Conference

UAE, Regional Cybersecurity Week

UAE, GISEC 2023

Thailand - Kaspersky Security Analyst Summit 2023

UAE, GITEX 2023,

Attending the National Day of People with special needs at Talal Abu Ghazaleh International Group (**TAG**) Knowledge Forum

5.4.3 Achievements

Launching LMS which is a dedicated training platform for employees in the government sector to qualify and educate them about the best security practices

Training and qualifying 30 students and graduates from Jordanian universities in each iteration of the Cyber Nashama camp

3,885 male and female students were trained on CTF trainings

Launching an awareness campaigns dedicated to people with special needs with the aim of spreading awareness about the most important security practices and warnings in the world of cybersecurity

Series of training sessions covering several sectors from the government, academic, and private sectors all over the kingdom

Training employees in the government sector to apply best practices on how to achieve the required cybersecurity levels that will be consistent with the Jordanian national cybersecurity framework

Launching '*Cyber Story*' Podcast that discusses many cybersecurity topics by hosting experts and professionals in the field

Launching several awareness campaigns such as: '*Digital Hint*' and '*Communicate Safely*'

5.5 2024 PLANNED ACTIVITIES

Efforts to make NCSC an accredited centre, locally and internationally, to issue licensing certificates related to cybersecurity services, providers, and products

Establishing a national cybersecurity academy that simulates best methods and latest technological tools and contribute to raising capabilities and developing skills

Strengthening the resilience of national institutions, CII sectors, and sensitive digital services in the Kingdom, and the ability to confront cybersecurity threats and incidents

Enhancing cybersecurity protection for national institutions by continuously building monitoring capacities for all government institutions

Developing advanced cybersecurity capabilities that stimulate the economy and supports the national security of the Kingdom

Building awareness and educational programs to enhance the protection of individuals on the Internet

Supporting and encouraging innovation to build high-level and sophisticated cybersecurity products and services

Strengthening international cooperation to benefit from global expertise in the fields of cybersecurity

Holding Dot Cyber Summit 2024 in it's 2nd iteration

Unit of Financial Computer Emergency Response Team - Jo-FinCERT

5.1 ABOUT THE ORGANIZATION

5.1.1 Introduction

Jo-FinCERT is the Financial Sector CSIRT. This unit oversees all Digital Forensics and Incident Response (**DFIR**) activities. Jo-FinCERT' s mission is to support and protect the financial institutions and its business, interests, and reputation from any kind of cyber-attacks

5.1.2 Establishment

The unit was established on the 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

5.1.3 Resources

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

5.1.4 Constituency

Jo-FinCERT is a sector centric CERT constituency being the financial and banking sectors in Jordan, namely banks, exchange companies, payment institutions, insurance, and microfinance institutions that are under the supervision of the Central Bank of Jordan

5.2 HIGHLIGHTS OF 2023

5.2.1 Summary of Major Activities

Manage sector-centric malware information sharing platform

Developing the non-Banking Financial Institutions Cybersecurity framework

Monitor the financial institutions digital assets

Conduct cybersecurity risk assessments, gap assessment, and remediation plans for the financial

institutions according to the Cyber Security Framework (**CSF v1.0**)

Joining FIRST

Joining TF-CSIRT

Conduct awareness sessions for financial institutions employees

Develop a guideline for financial consumer about financial fraud using electronic means

Generate regular CTI Reports about latest vulnerabilities and cyber-attacks techniques

5.3 ACHIEVEMENTS

Jo-FinCERT has implemented a number of strategic projects to enhance the cybersecurity capabilities of financial and banking institutions in Jordan

These projects include

- Developing a framework for information sharing and analysis
- Establishing a platform for automated threat intelligence sharing
- Collaborating with international organizations and response teams
- Developing a framework for protecting email systems
- Implementing a Domain Name System (**DNS**) framework

The Unit has also worked to improve Jordan's ranking in the ITU Global Cybersecurity Index (**ITU-GCI**)

In addition, Jo-FinCERT has conducted maturity level assessments, gap assessments, and remediation plans for the financial and banking institutions

Jo-FinCERT also monitors the security posture of financial and banking institutions and provides awareness training to employees

Overall, the Cyber Security Incident Response Unit for the Financial and Banking Sector has made significant progress in enhancing the cybersecurity of Jordan's financial sector

5.4 ACTIVITIES & OPERATIONS

5.4.1 Events organized by the organization/ agency

Jo-FinCERT organized a meeting with the managers of cybersecurity, compliance and risks from the banking sector on the 5 Jul 2023 to discuss the latest achievements Jo-FinCERT and address the future plans and initiatives

5.4.2 Events involvement

Jo-FinCERT participated in the following events and programmes

High Level Fintech Technical Committee Workshop

GITEX Technology Week 2023

Cyber Risk Quantification

Annual Administrative Leadership Forum

Secure, Monitor, and Manage your Future

Assessing the money laundering and terrorist financing risks associated with virtual assets

Crypto-assets' ecosystems in the international landscape

A workshop to study and analyse the market gap in the field of financial technology and innovation in the financial and banking sector and the main upcoming priorities

The first workshop of the Up-to-Date project

Operational risk system workshop

Assessing the risks of applications to join the regulatory laboratory

Electronic Crime Research

'*Foreseeing the Future*'

2023 Cybersecurity Workshop: *Cyber Resilience- Delivering Through Disruption*

A training program for the Threat Intelligence Platform

Conference '*Decision Makers and Criminal Justice Professionals*'

Cybersecurity for Central Bank Digital Currencies

ISO 27001: Lead Implementer

Convergence 2023

Financial technology and innovation

Induction program for newly appointed employees

'*Knowledge Session and Dialogue about Open Finance*'

AIDTSEC Conference and Exhibition

Information Security Management Systems ISMS-LI

Security Fundamentals

ISO 27001: Lead Implementer

Introduction to Business Innovation

Central Bank Cyber Resilience Workshop

2023 FIRST & AfricaCERT Symposium: Africa and Arab Regions

National Framework Implementation

F5 Conference

Cyber Intelligence Foundations

Cybersecurity by the Experts

National Framework Audit

Trellix Threat Intelligence Workshop

Black Hat MEA 2023

Penetration and detection of advanced smartphone vulnerabilities

5.4.3 Achievements

The unit sponsored the DOT Cyber Summit held in Jordan organize by NCSC

5.5 2024 PLANNED ACTIVITIES

Improving the information sharing platform

Revising the Information Sharing Framework

Financial Cyber Map for Banks

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.

6 KAZAKHTAN

NCS Kazakhstan - KZ-CERT

6.1 ABOUT THE ORGANIZATION

6.1.1 Introduction

The National Computer Emergency Response Team (**KZ-CERT**) is a single centre for the national information systems users and Kazakhstani Internet segment providing collection and analysis of cyber incidents report as well as consultative and technical assistance to Kazakhstani users in prevention of cyber threats

6.1.2 Establishment

KZ-CERT was established in 2011 as a republican state enterprise with the right of economic management '*Center for Technical Support and Analysis in Telecommunications*'

On 28 Jan 2013, the government of Kazakhstan adopted a decree to rename the republican state enterprise with the right of economic management '*Center for Technical Support and Analysis in Telecommunications*' as the republican state enterprise 'State Technical Service' with the mandate for economic management. In 2020, the RSE on REM[3] '*State Technical Service*' had undergone final reformation into the joint-stock company '*State Technical Service*' (hereinafter – **STS JSC**) by another governmental decree

In 2017, there was also an establishment of the National Coordination Center for Information Security (**NCCIS**) combining the operation of both KZ-CERT and the Government SOC

6.1.3 Resources

NCCIS, which is a structural subdivision of STS JSC, currently employs more than 60 people of various profiles. KZ-CERT Team, as a unit of NCCIS, comprises of 20 employees

[3] Republic State Enterprise on the Right of Economic Management

6.1.4 Constituency

KZ-CERT team's constituency are government, private and public sectors, every host or subnet related to the Kazakhstani Internet segment

6.2 HIGHLIGHTS OF 2023

6.2.1 Summary of Major Activities

In 2023, KZ-CERT Team members organized lectures, webinars, workshops, cybersecurity trainings for the government agencies, quasi-government organizations and various companies in Kazakhstan. The program involved presentations of the following topics

- '*Main Aspects of Information Security*'
- '*Cyber Hygiene Basics*'
- '*The Tricks of Cyber Fraudsters - How Not to Get Caught on Their Hook?*"
- '*Cyber-attacks Trends. International Cases*'

KZ-CERT Team members also contributed to raising awareness on cybersecurity through the national television. Accordingly, several appearances were made with the following presentations

- 'Combating *Fraud on the Internet*'
- 'Current Information Security Threats'
- 'Cyber Hygiene'

As part of the ongoing activities to cover the cybersecurity issues in the country, dedicated meetings involving the government agencies of Kazakhstan are also held regularly to discuss matters related to strengthening the level of information security in these organizations that play a significant role in domestic policy

KZ-CERT consistently inform the citizens on detected security incidents, potential and perceived computer security threats, as well as on the necessity of taking measures to eliminate, mitigate, and prevent such threats. The official website of KZ-CERT (*cert.gov.kz*), along with the newsfeed, features regularly published articles with recommendations on cyber hygiene and cybersecurity

All materials are usually provided in three languages – Kazakh, English, and Russian

For instance, the following articles were published in 2023

'*Microsoft: Exchange Server 2013 Support Service will end in 90 days*'
cert.gov.kz/news/13/2297

'*Recommendations for companies using Geoserver Software*'
cert.gov.kz/news/13/2356

'*Over 17 thousand routers in Kazakhstan are potentially vulnerable to Mikrotik RouterOS Vulnerability*'
cert.gov.kz/news/13/2413

'*Recommendations for protecting Whatsapp and Instagram accounts with 2FA*'
cert.gov.kz/news/13/2455

'*Technical details: Analysis of SSL/TLS cipher suites in the national top-level domain zone .kz*'
cert.gov.kz/news/13/2460

'*Important information for 1C-Bitrix CMS users*'
cert.gov.kz/news/13/2465

'*Vulnerability in all versions of Exim – no patch yet*'
cert.gov.kz/news/13/2471

'*Cisco vulnerability*'
cert.gov.kz/news/13/2475

'*Recommendations on protecting Telegram accounts*'
cert.gov.kz/news/13/2480

'*Recommendations for the users of Citrix products*'
cert.gov.kz/news/13/2491

'*How to be safe during Black Friday: KZ-CERT recommendations*' (available in Russian)
cert.gov.kz/news/13/2524

'*Recommendations for the users of Microsoft Office Professional Plus 2019 Excel*' (available in Russian)
cert.gov.kz/news/13/2538

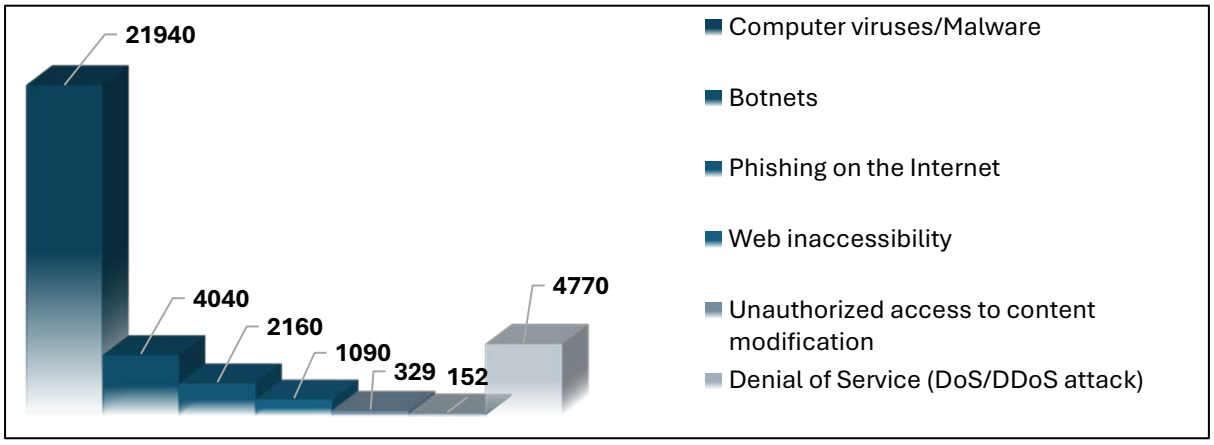
'*Frequent fraudulent cases on Whatsapp*' (available in Russian)
cert.gov.kz/news/13/2543

'*Information for the users of PostgreSQL*'
cert.gov.kz/news/11/2522

'*Two-factor authentication is an extra layer of security*'
cert.gov.kz/news/11/2457

6.2.2 Achievements

In 2023, KZ-CERT has handled over 34,000 cybersecurity incidents. Most incidents are associated with the creation and distribution of malware. The following diagram shows detailed information on the types of incident



Types of the incidents handled by KZ-CERT over 2023

- **2023 Cybersecurity Incident Case Example**

In 2023, KZ-CERT Team received a request from a Kazakhstani government agency to provide assistance in investigating a cybersecurity incident

During the examination of an affected laptop's disk image, several malicious

software types were detected inside – a botnet, a Trojan, and the CrazyCryp ransomware. Malicious files were found in the '*Workpace\metadata\FluidVoid\bin\Debug\Рабочий\готовые*' directory as well

KZ-CERT carried out the procedures of localization and neutralization of the malware software and prepared recommendations on preventing similar threats in future

The following table shows the detail of the malicious files

NO	FILENAME	SHA1 base32
1	\FluidVoid\bin\Debug\Build0_2.ex_	622RHQGQC3PEOTJV5J7TKIDQTW2GFXRO
2	\FluidVoid\FluidVoid\bin\Debug\Build1_2.ex_	HMX7VHMIIEEAKSMWIUJVJH74ICV67XII
3	\FluidVoid\FluidVoid\bin\Debug\Build0_1.ex_	U4YILJVTG3TRNABZGEHEXSU6N2IU4HAJ
4	\FluidVoid\FluidVoid\bin\Debug\Build0_3.ex_	JEFJSVL76PZODZRB6MLYYNAAOUZREKEJ
5	\FluidVoid\FluidVoid\bin\Debug\Build4_3.ex_	AFKGBUKDMOTFLYYZN7HQU7SOYEV26365
6	\FluidVoid\FluidVoid\bin\Debug\Build4_1.exe	WBF4YCELRKJJGPQQ3AGHGVXDRAN3RIAA
7	\FluidVoid\FluidVoid\bin\Debug\Build1_1.ex	WQD2P5IBZ4Z5CWZKRDRW23ANMRPYASHN
8	\FluidVoid\FluidVoid\bin\Debug\Build1_3.ex	2YQBHSSYLBLYTNINNITQO2AK6PPOAEQU
9	\FluidVoid\FluidVoid\bin\Debug\154.exe	Y52J4TNFQFV7GJ4SQGW4EGTYNYUOOROK
10	\FluidVoid\FluidVoid\bin\Debug\Build4_2.ex_	R5JHGHRJCNCXO45JOJCSTUENL5KKCFMC
11	\FluidVoid\FluidVoid\bin\Debug\llvann49.ex_	YVGI2MNXPXXPW2SOAPWOYYJ3OX3VYIFL
12	\FluidVoid\FluidVoid\bin\Debug\OvKSMx860.dll	332BIF6PBV34BDG5NTT34ORKJAFK74ZB
13	\FluidVoid\FluidVoid\bin\Debug\p2BBDVx861.dll	73DNKK5G2KZRBVOSDOKRPDCV76DLXODD
14	\FluidVoid\FluidVoid\bin\Debug\QHT4XDx861.dll	QOU2LFK7S4ZCWCBL4SWOXDJQ2SSF4FGE
15	\FluidVoid\FluidVoid\bin\Debug\Qa0mruyx860.dll	IMFHNRMFWGYSOOUZSIF743HAVY7UBBWT
16	\FluidVoid\FluidVoid\bin\Debug\Osiris_auto2.ex_	2JCU5NPBR7MWCXVDXRSPRWLXUTRBNWUC
17	\FluidVoid\FluidVoid\bin\Debug\t4me9m863.dll	77DLHTQBPL6XVDJUBVKNL4RISNNVJCBD
18	FluidVoid\FluidVoid\bin\Debug\vidar_business10.ex_	YJFTUKSPHBLHUJADL4TZFLSBNK2MKZKD
19	\FluidVoid\FluidVoid\bin\Debug\Cuddling36.ex_	ZVTSB7NJHSEEZZGQM4YUTQ35UOKDWSBV

6.3 ACTIVITIES & OPERATION

6.3.1 Events Involvement

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

International cooperation plays a big role in establishing communications with the global IT and cybersecurity communities, circulating important information, as well as maintaining the

status of a national computer emergency response team on the global stage through the participation in different international information security conferences and other events

- **Cyber Drills and Trainings**

OSCE Sub-regional training event on cyber/ ICT security

In May 2023, KZ-CERT Team members participated in the sub-regional trainings on cybersecurity and ICT security as representatives of Central Asian countries and Mongolia. The event was organized jointly with the Organization for Security and Co-operation in Europe (**OSCE**) and the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan, with the support of the United Kingdom. These trainings have become an important platform for international cooperation aimed at ensuring cybersecurity and the development of ICTs in the region

- **CTF Cyber Kumbez at the 'KazHackStan-2023'**

13 – 15 Sep 2023 Almaty, Kazakhstan - held a CTF event at the CyberKumbez cyber range, that had 24 Kazakhstani teams as participants

The purpose of the Cyber Kumbez CTF was to detect vulnerabilities in the exclusively designed infrastructure of a virtual city and simulate unacceptable events (business risks)

- **Kuban CTF at the IV 'Kuban CSC-2023' International Conference on Information Security**

12 - 13 Oct 2023 Sochi, Russia – held the IV International Information Security Conference Kuban CSC 2023 in the territory of the Krasnaya Polyana resort

Traditionally, this conference organized the final of the Kuban CTF-2023 practical information security championship, in which KZ-CERT Team also took part

- **11th Regional Arab, CIS, OIC-CERT Cyber Drill**

9 – 10 Oct 2023 – participate in the cyber trainings and workshops as part of the 15th OIC-CERT Annual Conference. KZ-CERT formed a team of 3 employees to participate in the event.

The OIC-CERT Cyber Drill, parts of which were independent of each other, was conducted on online platforms such as cyber task and cyber rangers

6.4 ACHIEVEMENTS

Every year KZ-CERT maintains efforts to conclude agreements with strategically important partners in the field of cybersecurity in order to formalize mutually beneficial cooperation in responding to threats and incidents of information security. Thus, in 2023, KZ-CERT has concluded one MoU in the field of cybersecurity

KZ-CERT Team members also actively attended various international conferences and meetings such as the following

Phuket, Thailand - Security Analyst Summit as speaker

Moscow, Russia - '*Infoforum-2023*' event as speaker

Moscow, Russia - '*Positive Hack Days 2023'* cyber festival as participant

Moscow, Russia - Annual '*SOC-Forum 2023*' event as participant

Montreal, Canada - 35th Annual FIRST Conference & NatCSIRT 2023 meeting as participant

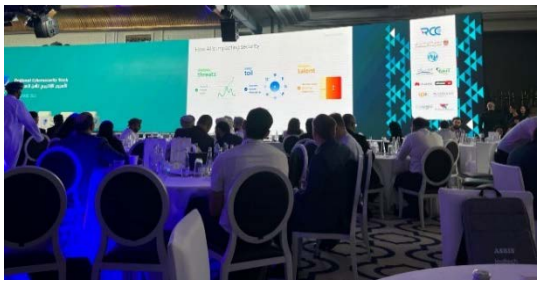
Almaty, Kazakhstan - Annual "*KazHackStan 2023*" conference as speaker

Berlin, Germany - FIRST Cyber Threat Intelligence Symposium 2023 as participant

CAMP 8th Annual Meeting 2023 as participant

Abu-Dhabi, UAE - 15th Annual OIC-CERT Conference and Regional Cybersecurity Week 2023 as participant

Tashkent, Uzbekistan - '*National Cyber Incident Classification*' workshop as speaker



7 KYRGYZ REPUBLIC

Cyber Security Center of Ala Too International University - CSC-AIU

7.1 ABOUT THE ORGANIZATION

7.1.1 Introduction

The Cyber Security Center of Ala-Too International University (**CSC AIU**) is acting as an academic computer emergency response team and centre for research and education in cybersecurity field

At the same time CSC AIU provides cybersecurity service to other universities, colleges, schools, and educational organizations to understand cybersecurity and develop cybersecurity teams, support the state organizations to improve cybersecurity awareness and capacity building CSC AIU collaborate with other international organizations and participate in international programs in developing digital skills and in field of cybersecurity

7.1.2 Establishment

CSC AIU was established on 11 Jan 2023 based on the Decision of the Academic Council of Ala-Too International University adopted on 29 Dec 2022

7.1.3 CSC AIU Constituents

CSC AIU has cooperation and close relationship with the state agencies (especially with the State Agency for Personal Data Protection under the Cabinet of Ministers of Kyrgyz Republic, Coordination Center of Cyber Security),

international and private organizations, and academia

7.2 HIGHLIGHTS OF 2023

7.2.1 Events involvement

20 Mar – 10 Apr 2023, USA - The CSC AIU representatives participated in the International Visitor Leadership Program (**IVLP**) Program "*Promoting Cybersecurity*" organized by the US Department of State

12 -14 Jun 2023 Tatarstan, Russia - The CSC AIU within the international cooperation on cybersecurity participated in the Digital Skills 2023 International training and cyber drill held in Kazan

13 14 Sep 2023 Almaty, Kazakhstan - Participation in KazHackStan International Cybersecurity Conference

11-12 Jul 2023 Tashkent, Uzbekistan - The CSC AIU took part in the international workshop '*Cyber 9/12 Strategy Challenge*'. Event was organized by OSCE in partnership with the US Department of State and MITRE Corporation

7.2.2 Events organized by CSC AIU

CSC AIU conducted a workshop and training on cybersecurity essentials and cyber hygiene for school teachers. AIU cares about improving of qualifications of teachers in secondary schools, particularly those located in remote regions of the country

20 Dec 2023 - the CSC AIU together with the State Agency for Personal Data Protection under the Cabinet of Ministers of the Kyrgyz Republic conducted CyberPro training for state and municipal employees

7.3 2024 PLANNED ACTIVITIES

Develop and establish academic Cyber Drill Platform for improving practical trainings for national universities, schools, and other stakeholders

Develop educational program on cybersecurity and cyber hygiene for primary schools

Establish the Cyber Security Club for AIU students with the appropriate infrastructure within the Cyber Security Centre to provide them with practical trainings and strengthening international cooperation with students' clubs and cybersecurity communities in other countries

8 LIBYA

National Information Security and Safety Authority - NISSA

8.1 ABOUT THE ORGANIZATION

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

8.1.1 Introduction

The National Information Security & Safety Authority (**NISSA**) is the umbrella of the Libya-CERT
nissa.gov.ly
www.facebook.com/nissa.libya

8.1.2 Establishment

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

8.1.3 Resources

70 employees

8.1.4 Constituency

National: Private & public sectors

8.2 ACTIVITIES & OPERATION

8.2.1 Events organized by the organization/ agency

- *30 Jan 2023* Tripoli, Libya - NISSA provide honorary sponsorship for the International Conference on Cyber Risks held in Corinthia Hotel. NISSA participated in the activities of the first day of the conference in two discussion sessions on the technical and legislative axes
- *25 Dec 2023* - A workshop entitled '*Professional Diploma Programs in Law and Informatics*' was sponsored by NISSA & shared with the Libyan Academy for Postgraduate Studies in the Tripoli Hall of the Bab Al Bahr Hotel. The event announce the launch of the diploma, which comes within the framework of supporting institutions and building administrative units for information security of each institution. It

also helps in localizing the cybersecurity industry and keeping pace with technological development. To create competencies capable of dealing with advanced technologies and the risks associated with them

8.3 HIGHLIGHTS OF 2023

8.3.1 Summary of Major Activities

The main task of NISSA is generally to protect the CII and respond to incidents and cyber-attacks targeting this infrastructure. Thus, by developing regulatory and legislative frameworks will enhance information safety to ensure the safe use of ICT

NISSA is working to localize the cybersecurity industry within institutions by helping these institutions secure their infrastructure as a first step towards digital transformation. NISSA has been working since the start to open channels of communication with all government and private institutions to spread the culture of cybersecurity

8.3.2 Achievements

The National Cybersecurity Strategy was approved by the Director General of NISSA in accordance with Resolution No. (05-2023). This strategy has been uploaded to the ITU website at *https://nissa.gov.ly/rujubij/National_CyberSecurity_Strategy_Layout_2022_A4-1.pdf*

NISSA was a member of a committee involved in preparing the first draft of the cyber-crimes law & the digital transaction law; these laws were approved as (05-2022) & (06-2022) laws by The Libyan House of Representatives, they have been published and in operation since 16 Jan 2023

In implementing NISSA's supervisory role over the cybersecurity service providers of the private sector, as a regulatory measure, NISSA has developed and approved a mechanism for obtaining permission to get cybersecurity services information from companies and individuals. The Director General of NISSA approved this mechanism in accordance with Resolution (36-2023) and coordination was made with the Ministry of Economy & Commerce as the body that grants licenses to provide such services

Activating Libya's membership in '*Women in Cyber Security Middle East*' group through NISSA's membership in OIC-CERT

In cooperation with the Libyan Academy for Postgraduate Studies, NISSA prepared a professional diploma in law and informatics, which is linked to the laws of electronic transactions and combating cyber-crime, in addition to national policies for information security and integrity

NISSA addressed the organization's secretariat with '*The National Policy Guide for Information Security and Safety*' in the 2nd edition. The document was uploaded to the organization's website as a guideline that establishes the cybersecurity policies enforce in the Libyan state

Feb 2023 - MoU & Non-Disclosure Agreement (**NDA**) were signed with Electronic Technology College – Tripoli, affiliated to the Ministry of Technical and Vocational Education, to cooperate in the field of information security

May 2023 - A cooperation agreement was signed between NISSA and the National Council for Economic and Social Development to activate the bilaterial cooperation in the areas of information security

31 Dec 2023 - MoU signed between NISSA and the Administrative Control Authority to cooperate in the fields of cybersecurity

17 NDAs were signed by NISSA with various government and private agencies. This is the first step towards activating bilateral cooperation and providing cybersecurity services to the benefit these agencies

'*Essential Cybersecurity Controls Checklist*' has been designed to be used during the inspection processes performed by NISSA on the cybersecurity CII of the government sector

2023 - NISSA launched the Public Key Infrastructure (**PKI**) Certificate Policy ver. 1.0 policy as a basis for the digital transformation of the Libyan state

NISSA launch the policy of using social media platforms at work in the government sector

A package of cybersecurity policies included in '*The National Policy Guide for Information Security and Safety*' was updated for the 2nd edition. NISSA took this action as a first step to prepare for the launch of the 3rd edition of this guide

2023 - NISSA launched '*Threats Exchange Platform*' to share cyber threats within the government sector

NISSA is a member on the Digital Lab. Team; The Digital Lab team consists of representatives from many vital government institutions in Libya that directly relate to digitization, technology, and innovation. It was established as an initiative supervised by the General Information Authority and supported technically by international experts through the E-NABLE project funded by the European Union and implemented by expertise from France

Events involvement

22 Feb 2023 - NISSA participated in the celebration ceremony of the '*Young Innovators Exhibition and Competition*' organized by the College of Electronic Technology – Tripoli. In the presence of the Minister of Technical and Vocational Education

14 - 15 Mar 2023 - NISSA was a coordinator and participant in the workshop on cybersecurity, which was organized by the Training Department of the General Staff of the Libyan Army. It was under the slogan '*The Dimensions and Risks of Cyberspace, Its Impact on the Military Institution and the Role of the Training Department*'. NISSA team participated by a presentation on the NISSA's competencies and major achievements

13 – 15 Feb 2023 - the University of Oxford, in cooperation with the General Communications and Informatics Authority and NISSA, organized a workshop in Tunis, Tunisia on assessing the cybersecurity situation in Libyan institutions. Parties from the public and private sectors participated in this workshop

1 Jun 2023 - NISSA participated in the activities of the 'National Technology Day', which is celebrated on the first of June every year. NISSA team provided awareness lectures and training workshops

Nov 2023 - NISSA participated in the activities of the International Libyan Conference on Information and Communications Technology (**ILCICT**), at the Corinthia Hotel, Tripoli. Many research papers and scientific lectures

were presented with regards to computer systems, informatics, communications systems, image processing, computer vision, and Internet of Things (**IoT**). The Director General of NISSA gave a presentation in which he summarized the most important activities and services and the most important cyber threats to which various institutions and entities are exposed. NISSA team also participated in the exhibition accompanying the conference

5 - 6 Dec 2023 -NISSA received an invitation from the Arab Information & Communication Technologies Organization (**AICTO**) to attend the Arab Cybersecurity Days activities in Tunis, Tunisia. It was organized within the framework of continuing supporting process to enhance joint Arab action and inter-regional and international cooperation in the field of developing digital trust and cybersecurity to ensure the success of technological transformations in the Arab region. The Director General of NISSA participated in these events. He was one of the prominent speakers at this event.

15 - 16 May 2023 - NISSA participated in a workshop promoting economic reform in Libyan ICT at Tobacts Hotel, Tripoli. This workshop was sponsored by the Internal Investment Authority. The work of this workshop focused on studying the extent of the maturity of institutions and the economic growth occurring in them and the relationship between the growth with ICT

8 Jun 2023 - A delegation from the office of the Communications and Informatics Authority in the Eastern Province, headed by the Director of the Electronic Services and Sector Development Department, visit NISSA HQ. During this visit, it was agreed on establish a bilateral cooperation, and initially NISSA engineers were assigned to provide an intensive cybersecurity training course. The targets are IT engineers affiliated with the Authority's office in the Eastern Region

25 – 27 Jul 2023 - NISSA participated in a workshop entitled '*Cyber Information Security and Digital Transformation of Institutions*' sponsored by the General Information Authority and organized by the Aldaleel Araqamee for Information Technology and Geographic Systems and Oracle International Company held from in Tunisia

9 – 10 Oct 2023 - NISSA participated in a joint workshop with the Council of Europe regarding harmonizing national legislation to protect personal data. The workshop was held in Tunisia with participation from many national bodies and supervised by the National Council for Public Liberties and Human Rights

8 Nov 2023 - NISSA responded to an invitation to attend a workshop held by the Ministry of Justice. It was about establishing ways of cooperation in digital transformation at the Ministry's HQ

دولـــــة ليبيا
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات
رقم (5) لسنة 2023 ميلادي
بشأن إعتماد الإستراتيجية الوطنية للأمن السيبراني

مدير عام الهيئة الوطنية لأمن وسلامة المعلومات:
- بعد الاطلاع على الاعلان الدستوري الصادر في أغسطس 2011ميلادي وتعديلاته.
- وعلى الاتفاق السياسي الليبي الموقع بتاريخ 17 ديسمبر 2015 ميلادي.
- وعلى محرجات ملتقى الحوار الليبي المنعقد بتاريخ 9 نوفمبر 2020 ميلادي.
- وعلى القانون رقم (12) لسنة 2010 ميلادي باصدار قانون علاقات العمل ولائحته التنفيذية.
- وعلى قرار مجلس الوزراء رقم (28) لسنة 2013 ميلادي بشأن انشاء الهيئة الوطنية لأمن وسلامة المعلومات.
- وعلى اللائحة الادارية للهيئة العامة للاتصالات والمعلوماتية.
- وعلى قرار وزير الاتصالات والمعلوماتية رقم (52) لسنة 2013م بشأن اعتماد الهيكل التنظيمي للهيئة الوطنية لأمن وسلامة المعلومات وتعديلاته.
- وعلى قرار رئيس الهيئة العامة للاتصالات والمعلوماتية رقم (55) لسنة 2018 ميلادي بشأن تكليف بمهام.
- وعلى ما قرره مجلس النواب بتاريخ 10 مارس 2021 بمنح الثقة لحكومة الوحدة الوطنية.
- وعلى مكتاب السيد/ مدير مكتب المدير العام رقم (2/26) بتاريخ 2023/01/19 ميلادي.

قـــــــرر

المادة الأولى
يتم بموجب أحكام هذا القرار إعتماد الاستراتيجية الوطنية للأمن السيبراني بالدولة الليبية.

المادة الثانية
على كافة الوزارات والمقاطعات والجهات التابعة لها مباشرة إستراتيجياتها وفقا لأحكام الأهداف العامة للإستراتيجية الوطنية للأمن السيبراني المعتمدة بموجب أحكام هذا القرار لضمان أمن وسلامة معلوماتها وأصولها ضد التهديدات السيبرانية.

المادة الثالثة
يعمل بهذا القرار إعتبارا من تاريخ صدوره. وعلى كافة الجهات تنفيذه.

م. صلاح الدين ابوزيد التيبي
مدير عام الهيئة الوطنية لأمن وسلامة المعلومات

صدر في طرابلس بتاريخ 2 / 2 / 2023م ميلادي

info@nissa.gov.ly | +218 21 361 4277 | +218 21 361 4127 / +218 21 361 4115
www.cert.gov.ly | www.nissa.gov.ly

دولـــــة ليبيا
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات
رقم (36) لسنة 2023 ميلادي
بشأن إعتماد آلية الحصول على إذن تقديم خدمات الأمن السيبراني

مدير عام الهيئة الوطنية لأمن وسلامة المعلومات:
- بعد الاطلاع على الاعلان الدستوري الصادر في أغسطس 2011ميلادي وتعديلاته.
- وعلى الاتفاق السياسي الليبي الموقع بتاريخ 17 ديسمبر 2015 ميلادي.
- وعلى ما قررة مجلس النواب بتاريخ 10 مارس 2021 بمنح الثقة لحكومة الوحدة الوطنية.
- وعلى القانون رقم (12) لسنة 2010 ميلادي باصدار قانون علاقات العمل ولائحته التنفيذية.
- وعلى قرار مجلس الوزراء رقم (28) لسنة 2013 ميلادي بشأن انشاء الهيئة الوطنية لأمن وسلامة المعلومات.
- وعلى قرار رئيس الهيئة العامة للاتصالات والمعلوماتية رقم (55) لسنة 2018 ميلادي بشأن تكليف بمهام.
- وعلى قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات رقم (44) لسنة 2021 ميلادي بشأن اعتماد السياسات الوطنية لأمن وسلامة المعلومات.
- وعلى قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات رقم (5) لسنة 2023 ميلادي بشأن اعتماد الأستراتيجية الوطنية للأمن السيبراني.
- وعلى مكتاب مدير مكتب المدير العام رقم (2/605) بتاريخ 2023/08/17 ميلادي بشأن اعتماد مقترح آلية الحصول على إذن تقديم خدمات الأمن السيبراني.
- وعلى ما تقتضيه المصلحة العامة.

قـــــــرر

المادة الأولى
تعتمد آلية الحصول على إذن تقديم خدمات الأمن السيبراني من الهيئة والمدرجة المرفقة بأحكام هذا القرار.

المادة الثانية
تلتزم الشركات والأفراد الراغبين في تقديم خدمات الأمن السيبراني بالحصول على إذن مزاولة من الهيئة. كما تمنح الشركات العاملة في هذا المجال مدة ستة أشهر لتسوية أوضاعها وفق الآلية المعتمدة من الهيئة.

المادة الثالثة
تتولى وزارة الاقتصاد والتجارة إشراط حصول الشركات والأفراد الراغبين في تقديم خدمات الأمن السيبراني على إذن من الهيئة قبل منحهم رخصة مزاولة النشاط. وتمتنع عن تجديد أي ترخيص لهذه الشركات والأفراد إلا بعد تسوية أوضاعهم مع الهيئة والحصول على إذن منها.

المادة الثالثة
يعمل بهذا القرار إعتبارا من تاريخ صدوره. وعلى كافة الجهات المعنية تنفيذه.

م. صلاح الدين ابوزيد التيبي
مدير عام الهيئة الوطنية لأمن وسلامة المعلومات

صدر في طرابلس بتاريخ 8 / 24 / 2023 ميلادي

info@nissa.gov.ly | +218 21 361 4277 | +218 21 361 4127 / +218 21 361 4115
www.cert.gov.ly | www.nissa.gov.ly

8.4 ACHIEVEMENTS

13 Jul 2023 - NISSA is considered the point of contact for the ITU-GCI in Libya. Accordingly, the questionnaire for the index in its fifth edition (2023 edition) was filled & referred to the GCI team

Feb 2023 - NISSA contributed to the preparation of the Oxford University report on assessing the situation of Libyan institutions in terms of cybersecurity, which was prepared in accordance with the workshop held in Tunisia. Many Libyan governmental and private institutions participated

8.5 2024 PLANNED ACTIVITIES

NISSA is in the process of joining FIRST with the technical requirements being prepared

For 2024, NISSA seeks to hold a cybersecurity conference aimed at enhancing information safety in line with the government's trend towards digital transformation. NISSA is planning to hold an awareness campaign during the international awareness month in Oct. 2024

A national cyber drill is planned to be organized in 2024 involving most of NISSA's constituency

In 2024, NISSA plans to hold workshops with government institutions to help them develop their information security strategies in accordance with the National Cybersecurity Strategy issued by NISSA

In cooperation with the Libyan Academy for Postgraduate Studies, NISSA launched the Professional Diploma in Law and Informatics. NISSA is working on preparing the educational programs for cybersecurity in cooperation with the Ministry of Higher Education and the Ministry of Technical & Vocational Education

Through the MoU concluded with the Administrative Control Authority, NISSA will work to conduct security inspections on the information security policies & essential cybersecurity controls of all governmental institutions to ensure that these institutions follow what is stated in the Information Security and Safety Policies Manual issued by NISSA


م. خالد امبارك
البنية التحتية الوطنية
للمفتاح العام PKI
اليوم - 1 يونيو
فندق كورنثيا طرابلس، ليبيا
م. علي جليان
مركز عمليات الأمن السيبراني
SOC
اليوم - 1 يونيو
كلية تقنية المعلومات - مدينة الزاوية
م. مازن ضو
أمن وسائل التواصل الاجتماعي
اليوم - 1 يونيو
الهيئة العامة للاتصالات والمعلوماتية
الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority
قادة التقنية
Techleaders
1 يونيو | 10 صباحًا
فندق كورنثيا طرابلس، ليبيا
م. سمر الدبري
أهمية التوعية
في الأمن السيبراني
اليوم - 1 يونيو
الهيئة العامة للاتصالات والمعلوماتية
م. أحمد المعداني
من أجل بيئة تكنولوجية
آمنة لأطفالنا
اليوم - 1 يونيو
قسم الحاسوب - كلية التربية / جامعة طرابلس

9 MALAYSIA

CyberSecurity Malaysia

9.1 ABOUT THE ORGANIZATION

9.1.1 Introduction

CyberSecurity Malaysia is the national cybersecurity specialist agency under the purview of the Ministry of Digital Malaysia having the vision of being a globally recognised National Cybersecurity and Specialist Centre. The services provided are categorized as follows:

- Cybersecurity Responsive Services
  - Security Incident Handling
  - Digital Forensics
- Cybersecurity Proactive Services
  - Security Assurance
  - Information Security Certification Body
- Capacity Building and Outreach
  - Info Security Professional Development
  - Outreach
- Strategic Studies and Engagement
  - Government and International Engagement
  - Strategic Research
- Industry and Research Development
- Cybersecurity Pre-emptive Services

9.1.2 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 2023, with the restructuring of the government administration, CyberSecurity Malaysia was put under the purview of the Ministry of Digital Malaysia. CyberSecurity Malaysia is committed 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

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

- **Cyber999 Cyber Incident Reference Centre**

  The Cyber999 provides 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 are available at MyCERT's website at *https://www.mycert.org.my/portal*

  MyCERT's Cyber999 has responded to 5,917 incidents in 2023 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 Dec 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

9.1.4 Constituency

CyberSecurity Malaysia's constituency is the Internet users in Malaysia. Cybersecurity incidents within Malaysia that are reported either by the Malaysian public or international organisations will be resolved by assisting the complainants with the technical issues. 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

9.2 HIGHLIGHTS OF 2023

9.2.1 Summary of Major Activities

12-16 Mar 2023 Dubai, UAE - Participated in the OIC-CERT 5G Security Working Group (**WG**) Meeting and Activity Roll Out Event in conjunction with the Gulf Information Security Exhibition & Conference (**GISEC**)

16-18 May 2023 Cairo, Egypt - Participated in the OIC-CERT Promotion Programme and the Egyptian Cybersecurity & Data Intelligence System (**CDIS**) Conference & Expo

31 Jul 2023 Online - Organised the 'Webinar Serumpun - *Susah-Susah Cari Rezeki, Senang-senang Scammer Curi*'. Malaysia Edition in cooperation with the Indonesian National Cyber and Crypto Agency (**BSSN**), Cyber Security Brunei (**CSB**), and the Cyber Security Agency of Singapore (**CSA**)

16 Aug 2023 Online - Organised the APCERT Cyber Drill '*Digital Supply Chain Redemption*'

11-13 Sep 2023 Kyoto, Japan - Chaired the APCERT Steering Committee Meeting

8 Oct 2023 Abu Dhabi, UAE - Organised OIC-CERT Board Meeting 05/2023

9 – 10 Oct 2023 Abu Dhabi, UAE - Participated in the 11th Arab Regional Security Summit, OIC-CERT & CIS Cyber Drill

11 – 12 Oct 2023 Abu Dhabi, UAE - Participated in the 15th Annual OIC-CERT Conference & FIRST Symposium for Arab and Africa with the theme "*Cybersecurity Innovation and Industry Development*"

8 Nov 2023 Online - Chaired the APCERT Annual General Meeting

9 Nov 2023 Online - Participated in the APCERT Annual Conference 2023

4-6 Dec 2023 Shenzhen, China - Participated in the OIC-CERT WGs Activities 2024 Workshop

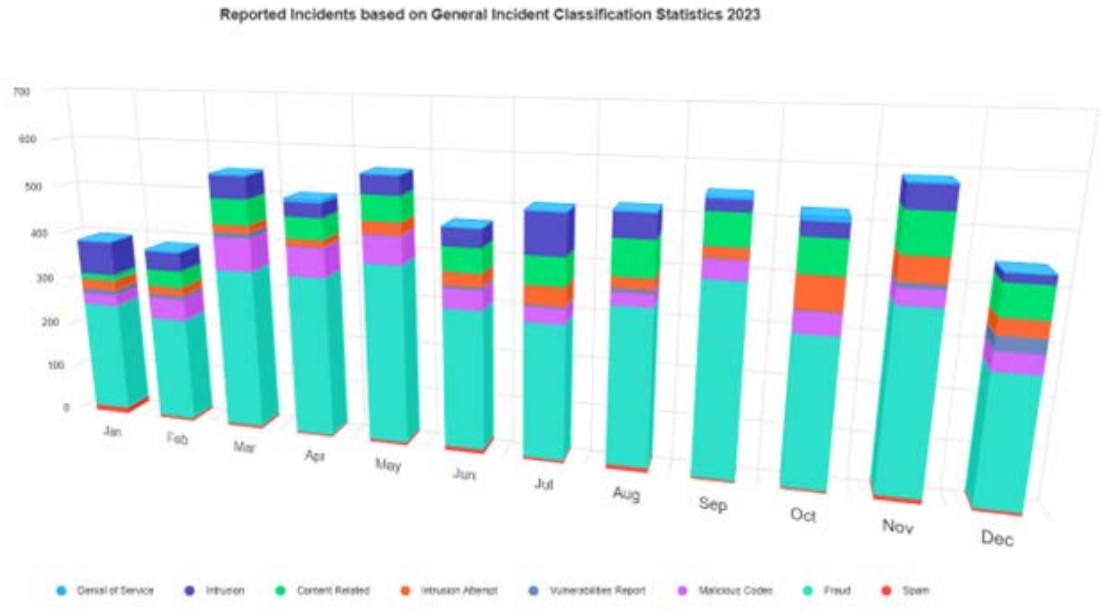
9.3 ACHIEVEMENTS

9.3.1 Incident Handling Reports and Abuse Statistics

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

CyberSecurity Malaysia, through MyCERT, had proactively produced 87 advisories and 17 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 intrusion. The following figure shows the reported incidents managed by MyCERT



More information on incidents reported to CyberSecurity Malaysia can be viewed at: *https://www.mycert.org.my/portal/statistics-2023*

9.3.2 Cyber Threat Research Centre

The centre operates a distributed research network for analysing malware and cybersecurity threats. The centre had also established collaborations 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

9.3.3 The LebahNET Project

The LebahNET is a Honeypot Distributed System where a collection of honeypots is used to study the exploits functioned and 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

LebahNET portal at *https://dashboard.honeynet.org.my/dashboard/12/2023*

Kibana portal at *https://es.honeynet.org.my/ by using guest authentication*

Username: guest

Password: guest2021!

9.4 ACTIVITIES & OPERATION

CyberSecurity Malaysia actively participated in cybersecurity events such as trainings, seminars, conferences, and meetings. Some of the major participations are as follows:

9.4.1 Cyber Drills

CyberSecurity Malaysia successful organised the APCERT Cyber Drill 2023 theme "*Digital Supply Chain Redemption*". The objective of the drill is to test on the procedures and incident handling practices of participating organisations. There were 28 Computer Security Incident Response Team (**CSIRT**) from 24 economies of APCERT and non APCERT members, 15 CSIRTs from 14 economies of OIC-CERT and AfricaCERT

Apart from the APCERT Cyber Drill, CyberSecurity Malaysia had also participated in two cross-national Cyber Drills namely the OIC-CERT and Arab Regional Cyber Drill 2023 and ASEAN CERT Incident Drill (ACID) 2023

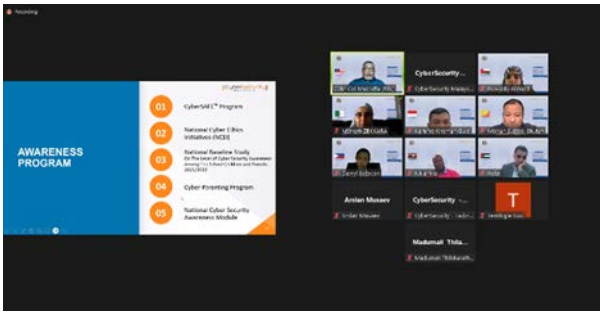
9.4.2 Trainings

Hands-on training such as the Digital Security Lifelong Learning Program (**DSLP**) under the Malaysian Technical cooperation Programme (**MTCP**) was conducted by CyberSecurity Malaysia from 13-16 &19-20 Jun 2023. There were 11 participants from Algeria, Bhutan, Eswatini, Indonesia, Jordan, Maldives, Nigeria, Philippines, Oman, Sri Lanka, and Uzbekistan

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 updated cybersecurity knowledge from domain experts and experience practitioners

MTCP Opening Ceremony



The MPCP Training

9.4.3 Presentations

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

14 – 16 Mar 2023 Dubai, UAE - As a speaker at the GISEC at the World Trade Center

16 -18 May 2023 Cairo, Egypt - As a speaker at the Egypt Cybersecurity & Data Intelligence System (**CDIS**)

5 – 7 Oct 2023 Tokyo, Japan - As a speaker at the conference entitled '*Collaboration for a Cyber-Safe ASEAN-Japan Community*' at the International Conference on ASEAN Japan Cybersecurity Community

9 Nov 2023 Online – As a speaker at the APCERT closed conference entitled '*Threat Analysis on Emerging Data Leakage in Malaysia from MyCERT Perspective*'

5 – 6 Dec 2023 Manama, Bahrain - As a speaker at the conference entitled "*Empowering Global Cooperation in Cybersecurity*" at the Arab International Cybersecurity Summit 2023

9.4.4 Research Papers

CyberSecurity Malaysia actively contribute research papers to journals and conference proceedings. Among the papers published

RENTAKA: Identifying Windows Cryptographic Ransomware based on Pre-Attack API Calls Features and Machine Learning Classifiers - Semarak Ilmu Publishing

*M-health digital evidence taxonomy system (**MDETS**): Enabling digital forensics readiness with knowledge sharing approach* - AIP Publishing

Systematic literature review: Trend analysis on the design of lightweight block cipher - Elsevier

Modified Generalized Feistel Network Block Cipher for the Internet of Things – MDPI

*The Systematic Literature Review on Information Security Culture (**ISC**) Research* - Institute of INFORMATICS

Understanding How National CSIRTs Evaluate Tools and Data: Findings from Focus Group Discussions - Association for Computing Machinery (**ACM**)

Ransomware Behaviour on Windows Endpoint: An Analysis - IPN Education Group Conference

Cryptographic Ransomware Early Detection using Machine Learning Approach and Pre-Encryption Boundary Identification - WAWM Academy, Semarak Ilmu

The National Cyber Ethics Modules: An Approach for Teaching Cyber Safety to K12 Students - International Academy of Technology, Education and Development (**IATED**)

9.4.5 Social Media

In 2023, 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 59,000 followers and the CyberSecurity Malaysia Twitter has 7,873 followers

9.4.6 Events

- **The 15th OIC-CERT Annual Conference 2023**

  11 - 12 Oct Abu Dhabi, UAE - The conference organized by ITU-ARCC in

cooperation with OIC-CERT, UAE Cyber Security Council, ITU, and FIRST with the theme '*Cybersecurity Innovation and Industry Development*'. Gen (R) Tan Sri Zulkifeli Mohd Zin, Chairman of Cybersecurity Malaysia and Dato' Ts. Dr. Haji Amirudin Abdul Wahab FASc were the speakers for the panel sessions "*Shaping the Culture of Innovation in Cybersecurity*" and "*National and Regional Cybersecurity Initiatives*" respectively

- **OIC-CERT Working Groups Activities 2024**

  CyberSecurity Malaysia participated and moderated the OIC-CERT WGs 2024 Planning Workshop in Shenzhen, China hosted by Huawei. The workshop discussed activities for the OIC-CERT 5G Security WG, Cloud Security WG, and other WG activities for 2024

9.5 INTERNATIONAL COLLABORATION

The Malaysia Cybersecurity Strategy 2020-2024 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

9.5.1 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

- Bangladesh e-Government Computer Incident Response Team (**BGD e-GOV CIRT**)
- Badan Siber dan Sandi Negara, Indonesia
- British High Commission Singapore
- National Revenue Authority (**NRA**) Republic of South Sudan
- Minister of Security, Republic of Uganda
- Tanzania Bank, Tanzania

9.5.2 International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia

The Permanent Secretariat of the OIC-CERT, where the major role is to undertake daily operations and facilitate

cooperation and interaction among the members countries

The lead for the Capacity Building Initiatives in the OIC-CERT business plan

Co-Lead the OIC-CERT 5G Security Working Group with the objective of developing a security framework to be adopted by the OIC member countries

The Chair of the APCERT

Member of FIRST

9.6 FUTURE PLANS

CyberSecurity Malaysia strives to improve the service capabilities and encourage local Internet users to report cybersecurity incidents to the Cyber999. 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 Memorandum of Understandings (**MoU**) and agreements

CyberSecurity Malaysia and Aerosea Exhibitions Sdn. Bhd will be organizing an international event known as the Cyber Digital Services, Defence and Security Asia (**CyberDSA'24**). This event is scheduled to take place 6 - 8 Aug 2024, at the Kuala Lumpur Convention Centre. To be held concurrently with this prestigious event are The Cybersecurity Malaysia ACE Awards (**CSM-ACE**) and Sibersiaga. The CSM-ACE 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.

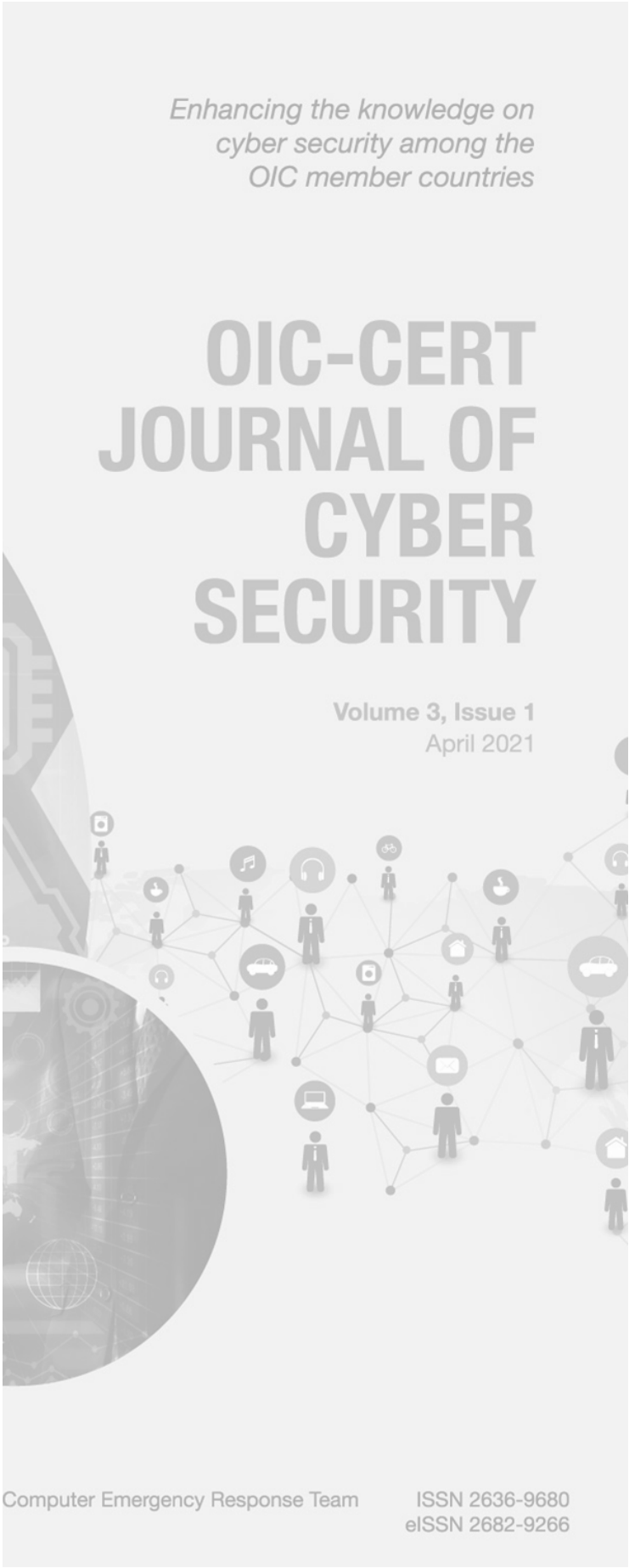
9.7 CONCLUSION

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

In line with the Malaysia Cybersecurity Strategy 2020-2024 that emphasized on capacity and capability building, mitigation of cyber threats, and

international collaboration, CyberSecurity Malaysia will continue to enhance existing and develop new cybersecurity processes, capabilities, and technologies. CyberSecurity Malaysia will also continue with the commitment to seek new edges in cybersecurity and to be a catalyst in developing the industry

International cooperation and collaboration are an important facet in mitigating other cybersecurity issues. As the cyber environment does not conform to the physical boundary of the countries, international relations will remain an important initiative. With the rapid development of the internet, the economies are now dependent on public network applications such as online banking, online stock trading, e-business, e-governments, and the protection of the various national information infrastructures. CyberSecurity Malaysia will continue to establish and support cross border collaboration through bilateral or multilateral platforms such as the APCERT and the OIC-CERT and will continuously pursue new cooperation with cybersecurity agencies regionally and globally in the effort to make cyberspace a safer place to carry out social and economic activities



10 NIGERIA

Nigeria And Consultancy Support Services Limited – CS2

10.1 ABOUT THE ORGANIZATION

10.1.1 Executive Summary

In 2023, Nigeria and Consultancy Support Services (**CS2**) Limited navigated a complex environment characterized by political shifts, economic volatility, and operational challenges. Amidst these conditions, CS2 demonstrated resilience, adaptability, and a forward-looking perspective, reaffirming its leadership in the cybersecurity and ICT policy consultancy sectors

10.1.2 Key Achievements

CS2 played a pivotal role in developing the Nigeria Civil Aviation Authority (**NCAA**)'s ICT and cybersecurity policies, marking a significant advancement in national aviation security and digital governance

CS2 efforts in change management and transformation at the NCAA Corporate Headquarters, alongside the implementation of EMPIC[4] software, underscored the commitment to digital transformation within the aviation sector

The completion of a comprehensive Security Audit for the National Digital Identity Management Systems (**NIMS**) Infrastructure highlighted our expertise in safeguarding critical digital assets and enhancing national security protocols

Participation in the APCERT Cyber Drill exemplified our engagement with global cybersecurity communities, reinforcing our dedication to international cybersecurity resilience and cooperation

10.1.3 Organizational Overview

Since its inception in 2002, CS2 has established itself as a premier consultancy in cybersecurity, capacity building, and ICT policy, offering a broad range of services to clients across Nigeria, Africa, and globally

[4] The Standard software for Aviation Regulators everywhere

The work spans multiple disciplines, emphasizing cybersecurity, information management, change management, and software development, serving a diverse client base that includes governmental and non-governmental organizations

10.2 OPERATIONAL HIGHLIGHTS

CS2's active involvement in global cybersecurity events and policy advisory roles has contributed significantly to shaping cybersecurity practices and frameworks across Africa

CS2 commitment to capacity building, legislative advocacy, and collaborative initiatives with government entities underscores the role in fortifying national and regional cybersecurity infrastructures

10.2.1 Future Directions

CS2 plans to deepen the involvement in international cybersecurity forums and enhance cyber-forensics capabilities, reinforcing leadership in cybersecurity excellence

The strategic focus will also include supporting synergies between military, civilian, and law enforcement sectors to strengthen national cybersecurity postures

Collaborative efforts with the government agencies are set to expand, aiming to elevate cybersecurity standards and practices within the national frameworks

Despite the year's challenges, CS2's dedication to promoting cybersecurity, digital resilience, and policy advocacy remained unwavering. The organization achievements in 2023 are a testament to the strategic vision and operational excellence. Looking ahead, CS2 is poised to continue its leadership role in shaping the cybersecurity landscape in Africa and beyond, driven by a commitment to innovation, collaboration, and capacity building. The proactive stance and contributions to national and global cybersecurity initiatives underscore the vital role as a catalyst for digital security and resilience

10.3 ANNUAL REPORT 2023

The following encapsulates CS2's journey through 2023, highlighting the adaptability, strategic achievements, and commitment to excellence in a changing world. CS2 ongoing efforts to advance cybersecurity and ICT policies reflect the dedication to enhancing digital safety and governance, positioning CS2 as a cornerstone of cybersecurity consultancy on a global scale

10.3.1 About Organization/ Agency

Introduction

CS2 is a Cybersecurity, e-Library, Organization Effectiveness/ Change Management, and ICT Policy Consultancy firm

Establishment

Consultancy Support Services Limited was incorporated on 13 Feb 2002

Resources

- Cybersecurity Specialist
- Project Implementation
- Change Management
- Library and Information Management Specialist
- Information Management and Systems Networking
- Change Management
- Computer Programming & Enterprising Management
- Digitization
- Archiving & Digital Libraries
- Computer Forensics & Cybersecurity
- Information Technology Infrastructure

Constituency

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

NCAA Participants Group Photograph during the Stakeolders' Retreat 2023

10.4 HIGHLIGHTS OF 2023

10.4.1 Summary of Major Activities

Facilitated the NCAA ICT Policy and Cybersecurity Policy successfully completed

Provision of Change Management for Transformation in NCAA Corporate HQ and across all its location (Ongoing)

Provision of Comprehensive Privacy and Security Audit of NIMS Infrastructure and Ecosystem for Nigeria Digital Identification for Development (**ID4D**) Project (2023 till present)

Asia Pacific Computer Emergency Response Team (APCERT) Cyber Drill (2023)

10.4.2 Achievements

The achievements of CS2 in 2023 are notable for their impact on national aviation security, digital governance, and the broader cybersecurity landscape. Following are the highlighted achievements

Development of NCAA's ICT and Cybersecurity Policies - CS2 played a critical role in formulating ICT and cybersecurity policies for NCAA marking

a significant advancement in the national aviation security and digital governance

Change Management and Digital Transformation at NCAA - CS2's efforts in change management and transformation at the NCAA Corporate HQ, along with the implementation of EMPIC software, underscored the commitment to digital transformation within the aviation sector

Security Audit for the National Digital Identity Systems - The completion of a comprehensive Security Audit for the NIMS Infrastructure demonstrated CS2's expertise in safeguarding critical digital assets and enhancing national security protocols

Curriculum Development - The completion of the curriculum for the Nigeria Higher National Diploma Cybersecurity for the National Board for Technical Education (**NBTE**)

Participation in the APCERT Cyber Drill: CS2's involvement in the APCERT Cyber Drill reinforced the dedication to international cybersecurity resilience and cooperation, exemplifying engagement with global cybersecurity communities

Cross Section of Participants during the APCERT Cyber Drill 2023

Players and Observers at the APCERT Cyber Drill 2023

Completed a NCAA ICT Policy and Cybersecurity Policy Stakeholders' Retreat

Continue to Chair and support the Nigeria Computer Society (**NCS**) Cybersecurity Advisory Group

Facilitated training activities such as the Executive Registration Programme (**ERP**) of the Computer Professionals Registration Council of Nigeria (**CPrN**) (2023).

These achievements reflect CS2's leadership in the cybersecurity and ICT policy consultancy sectors, demonstrating a strategic vision, operational excellence, and a commitment to advancing cybersecurity, digital resilience, and policy advocacy both nationally and globally

10.5 ACTIVITIES AND OPERATION

10.5.1 Events involvement

16 Aug 2023 Online - APCERT Cyber Drill (2023)

9 - 13 Jan 2023 Maitama, Abuja Nigeria- Participated in the Policy and Governance Advisory Committee

18 Jan 2023 Online - Participated in Cyber Podcast Series, European Commission

23 - 26 Jan 2023 Online - Nigeria Cybersecurity 2023 Perspective

30 Jan 2023 Online - Participated in making Africa Safe Advisory Board Members, CIBEROBS

6 Feb 2023 Abuja, Nigeria - Participated in the Nigeria Cybersecurity Submit 2023 '*Building a Secure Digital Future'*

7 - 9 Feb 2023 Washington DC USA - Participated in Global Conference on Cyber Capacity Building (**GC3B**)

21 - 23 Feb 2023 Johannesburg South Africa - Participated in 8th Edition of CISO Africa: '*Building a Robust and Resilience Security Community for Africa to help future proof'*

4 - 7 Mar 2023 Bouznika, Morocco - Participated in the International Conference Strengthening Cooperation on Cyber Crime and e-Evidence in Africa

14 - 16 Mar 2023 UAE - Participated in GISEC 2023 on Securing Critical Infrastructure and Strategies for Government Authorities

28 - 30 Mar 2023 Stellenbosch, South Africa - Participated in 3rd International Workshop on Combating Transnational Crime in Africa: '*The African Cyber Security Landscape Countering Cyber Threat Proliferation in Africa*'

11 - 12 Apr 2023 Abuja, Nigeria - Participated in Nigeria Data Protection & SRAP Validation workshop

14 Apr 2023 – present - Implementation of NIMC Privacy and Security Audit of NIMS Infrastructure and Ecosystem

25 - 26 Apr 2023 Abidjan - Participated in Cyber Africa Forum on 4th Industrial Revolution AI between Threat and Opportunities

1 - 5 May 2023 Abuja, Nigeria - Facilitated at NCAA Stakeholders' Retreat on ICT Policy and Cybersecurity Policies

Cross section of the Participants during the NCAA Stakeholders' Retreat 2023

10 - 12 May 2023 Abuja, Nigeria - Participated in the Nigeria Computer Society Cybersecurity Operations and Tactics: '*Leaving from International Experience'*

24 to 26 May 2023 Abuja, Nigeria - Facilitated in Consultations on the National Legal Framework for Cybercrimes

30 May - 1 Jun 2023 Marrakesh, Morocco - Participated in GITEX Africa 2023

6 to 15 Jun 2023 Johannesburg, South Africa –Participated in IT Web Security Summit 2023

16 - 17 Jun 2023 Abuja, Nigeria – Participated in Computer Professional of Nigeria (**CPN**) 2023 IT Professional Assembly

11 - 12 Jul 2023 Abuja, Nigeria - Participated in Cyber Secure Nigeria 2023 Conference '*Cybersecurity and Sustainability*'

18 to 19 July 2023 Kenya - Participated in CyFrica 2023

31 Jul - 4 Aug 2023 Tanzania - Participated in Africa Endeavour 2023

7 - 9 Aug 2023 South Africa –Participated in Crisis Management and Diplomacy in African Union Context Workshop

11 Aug 2023 Online - Participated in Global Conference on Cyber Capacity Building

Aug – Nov 2023 Nigeria Participated in the development of a curriculum for the Nigeria Higher National Diploma Cybersecurity for NBTE

29 Aug 2023 Abuja, Nigeria –Facilitated in Nigeria ACSS Alumni Chapter and George C. Marshall European Center for Security Studies (**GCMC**)

5 - 6 Sep 2023 Abuja, Nigeria - Facilitated in 16th Annual Banking and Finance Conference

12 Sep 2023 Abuja, Nigeria.- Participated in a joint platform for Advancing Cybersecurity in Africa, ECOWAS Commission

13 - 14 Sep 2023 Maputo, Mozambique - Participated in the Mozambique Banking, Financial Services and Insurance

26 to 29 September 2023 Algiers, Algeria- Participated in Regional Workshop on Countering the use of Cyberspace for Terrorist purpose, African Center for the Study and Research on Terrorism (**ACSRT**)

3 - 5 Oct 2023 – Addis Ababa, Ethiopia - Participated in the Overviews of Strengths, Weaknesses, Opportunities and Threats of African Cyberspace, ITU Regional Development Forum

9 - 13 Oct 2023 Abu Dhabi, UAE - Participated in 15th OIC-CERT Annual Conference of Regional Cybersecurity Week 2023

17 - 19 Oct 2023 Johannesburg, South Africa - Participated in the African Union Development Agency (**AUDA-NEPAD**)

07 - 09 Nov 2023 Abuja, Nigeria - Facilitated in Federal Ministry of Justice Cybercrimes Awareness Campaign

14 - 16 Nov 2023 Lagos, Nigeria - Facilitated in Legislative Reform on Cybercrime and Electronic Evidence

21 - 22 Nov 2023 Lagos, Nigeria - Facilitated in Central Bank of Nigeria/ FITC Directors Programme

29 - 30 Nov 2023 Accra, Ghana - Participated in GC3B

05 Dec 2023 Seoul, South Korea - Participated in the World Emerging Security Forum

13 - 15 Dec 2023 - Bucharest, Romania - Participated in AUC Octopus Conference

10.5.2 Profile Summary

Cybersecurity, Capacity Building, and ICT Policy Development 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.

10.6 PLANNED ACTIVITIES

Continuous involvement in

- OIC CERT
- Global Forum on Cyber Expertise (**GFCE**)
- African Union Cybersecurity Expert Group (**AUCSEG**)
- Global Commission on the Stability of Cyberspace (**GCSC**)
- Internet Corporation for Assigned Names and Numbers (#**ICANN**),
- NCS
- CPrN
- Cyber Security EXPERTS association of Nigeria (**CSEAN**)
- and related activities

Delivery of the Cybersecurity Landscape in Africa: Assessment of Gaps and Priorities Report as input into the African Cybersecurity Strategy

Completion of African Digital Compact and an African Common Position on the United Nations Global Digital Compact

Provision of training on Cybersecurity, Data Privacy & Protection for the Nigeria Bank of Industry (**BOI**) and other clients

Continuous in-house cyber-forensics capacity development program

Provide services in support of Military-Civilian, Law Enforcement and related Cybersecurity Initiatives

Collaborate with the Government Inter-Agency Committees on the implementation of Cybersecurity measures

Support the following national initiatives

- Implementation of the Nigeria Data Protection Policy

- Development of Higher National Diploma (**HND**) Cybersecurity Curriculum for NBTE
- Implementation of a Nigeria Data Protection Roadmap
- Harmonisation, standardisation, and seamless interoperability of national identity systems as well as evolving a Business Model/ Plan defining the rules of engagement governing access of Foundation Identity by Agencies/ organisations providing Functional national identity
- Development of the national frameworks and guidelines to protect the Nigerian IT systems from deliberate attack from internal and/ or external parties
- Development of the digital literacy and e-inclusion schemes for under-served communities, including women and girls
- Increase the compliance and adoption of IPv6 standards
- Strengthen the ICT departments in Higher Education Institutions (HEI)
- Development of a blueprint of common services, policies, standards, procedures, and technical components that guide Ministries, Departments, and Agencies on IT investment

10.7 CONCLUSION

As a reflection on the tumultuous yet transformative year of 2023, CS2 stands as a beacon of resilience, innovation, and strategic foresight. The journey through a landscape marred by political, economic, and operational upheavals underscores CS2 unwavering commitment to cybersecurity, digital resilience, and ICT policy development. The challenges of the past year, rather than deterring, have honed CS2 to resolve, catalysing significant advancements in national and global digital security landscapes

The key achievements, from spearheading critical policy formulations in the aviation sector to enhancing national digital identity systems, affirm CS2 pivotal role in shaping cybersecurity and digital governance. Participation in the global platforms like the APCERT Cyber Drill not only amplifies our voice in the international cybersecurity dialogue but also fortifies our networks, fostering collaborations that transcend borders

Looking ahead, CS2 is primed to further cement its status as a leader in the cybersecurity domain. Forward-looking agenda is replete with initiatives aimed at deepening engagement in international cybersecurity forums, augmenting cyber-forensics capabilities, and fostering synergies across military, civilian, and law enforcement sectors. This strategic blueprint is not merely a roadmap but a commitment to elevating cybersecurity standards, driving innovation, and nurturing a secure digital future

The resilience and achievements of CS2 in 2023 are a testament to the strategic vision, operational excellence, and tireless dedication of the team. As we pivot towards the future, CS2 sights are set on new horizons, driven by a commitment to innovation, collaboration, and capacity building.

The role as a catalyst for digital security and resilience is more critical than ever, as CS2 navigate the complexities of an increasingly interconnected world

This Annual Report 2023 encapsulates a year of challenges, triumphs, and relentless pursuit of excellence. CS2 remains steadfast in its mission to advance cybersecurity and ICT policies, poised to continue its leadership role in shaping the cybersecurity landscape in Africa and beyond. The journey is far from over; it is merely the prelude to greater achievements and deeper impacts in the realms of digital safety and governance. Together, CS2 forge ahead, determined to make an indelible mark on the global cybersecurity landscape, ensuring a safer, more resilient digital world for generations to come

NCAA Different Sydicates of ICT & CyberSecurity Policies Stakeholders' Retreat at Different Roundtables

NCAA Different Sydicates of ICT & CyberSecurity Policies Stakeholders' Retreat at Different Roundtables

NCAA Syndicate One Participants at ICT & CyberSecurity Policies Stakeholders' Retreat

NCAA Syndicate One Participants at ICT & CyberSecurity Policies Stakeholders' Retreat

Participants Group Photograph during the APCERT Cyber Drill 2023

Participants Group Photograph during the development of the Higher National Diploma CyberSecurity, 2023

11 OMAN

Oman National CERT – OCERT

11.1 ABOUT THE ORGANIZATION

11.1.1 Introduction

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

The ITU Arab Regional Cyber Security Center (**ITU-ARCC**), which was established by the International Telecommunication Union (**ITU**) and the Omani Government, represented by the Ministry of Transport, Communications and Information Technology (**MTCIT**),has a vision of creating a safer and cooperative cybersecurity environment in the Arab Region and strengthening the role of ITU in building confidence and security in the use of information and communication technologies in the region. In line with the objectives of the ITU Global Cybersecurity Agenda (**GCA**), ITU-ARCC act as ITU's cybersecurity hub in the region localizing and coordinating cybersecurity initiatives. ITU-ARCC is hosted, managed, and operated by OCERT

11.1.2 Resources

- *https://cert.gov.om/*
- *https://arcc.om/?GetLang=en*
- *https://arcc.om/pages/4/show/8*
- *https://rcssummit.com*/
- Alliances and Cooperation team at Oman National CERT
- ITU-Arab Regional Cyber Security Center team

11.1.3 Constituency

The Sultanate of Oman

11.2 HIGHLIGHTS OF 2023

11.2.1 Summary of Major Activities and Achievements

- **International Level**

11-12 Sep 2023 Beirut, Lebanon - Participated in a workshop on building trust in digital government services at the United Nations House, organized by the Arab Information and Communication Technologies Organization in collaboration with the United Nations Economic and Social Commission for Western Asia (**ESCWA**) and the Internet Society and the ITU-ARCC

9 Oct 2023 Abu Dhabi, UAE - The Sultanate of Oman, represented by MTCIT, chaired the 1st 2023 meeting of the Boards of OIC-CERT held in Abu Dhabi, United Arab Emirates

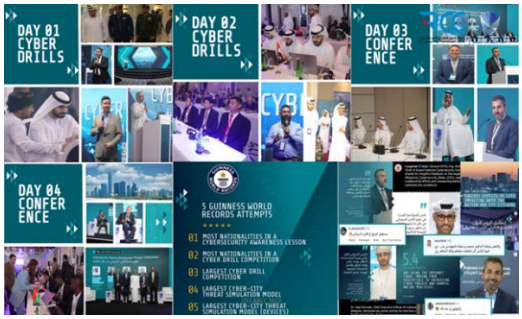
9 - 12 Oct 2023 Abu Dhabi, UAE - The ARCC organized the Regional Cybersecurity Week with the theme '*Innovation in Cybersecurity'* in cooperation with the ITU, FIRST, and the Cybersecurity Centres of the Organization of Islamic Cooperation. The event is hosted by UAE represented by the Cybersecurity Council. The week included

- The 11th Regional Cybersecurity Drill
- The 11th Regional Cybersecurity Conference
- The Board Meeting of the OIC-CERT
- The 11th Arab Cybersecurity Cooperation Team (**ACCT**) meeting for the Heads and Representatives of the National Cybersecurity Centres in the Arab Region
- FIRST workshop
- The 5th OIC-CERT Annual Conference
- The 2nd OIC-CERT Global Award 2022

The Regional Cybersecurity Week 2023 was awarded with 5 Guinness World Records, which are

- The largest simulation model of cybersecurity attacks with over 50 speakers
- The largest competition in simulating cybersecurity attacks with the participation of 11 international organizations
- The largest number of nationalities in a cybersecurity attack simulation competition with participants from over 30 countries
- The largest simulation model of cyber city threats
- The largest number of nationalities in a cybersecurity awareness lecture with over 500 attendees

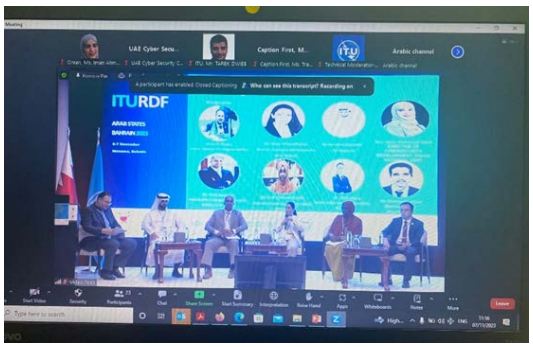
Presented the Cybersecurity Diplomacy Initiative in the Middle East of the United Nations (**UN**) a collaboration between the ARCC and the Human Dialogue Organization



6 - 7 Nov 2023 Manama, Bahrain - ITU-ARCC participated in the Regional Development Forum for Arab States (**RDF-ARB**), organized by ITU Telecommunication Development Bureau (**BDT**) and hosted by the Ministry of Transportation and Telecommunications

Riyadh, Saudi Arabia - The Head of the ARCC, Eng.Badar Al-Salhi, participated in a workshop titled '*Diplomacy and Cybersecurity: Trends, Innovations, and Challenges*', within the panel discussion on '*Building Trust Standards and International Cooperation in Cybersecurity*'

26 Oct 2023 - The Sultanate of Oman, represented by the MTCIT, participated via video conferencing in the second meeting of the Executive Committee for Cybersecurity in the Gulf Cooperation Council countries



16 - 20 Oct 2023 - Participation of the OCERT in GITEX 2023 through dialogue sessions on cybersecurity industry and its impact on the global economy

In support of women's role in cybersecurity, OCERT participated in JESSIC Global 2023 with a dialogue session on capacity building for cybersecurity workforce

Jordan - OCERT participated in the 1st Jordan Cybersecurity Summit organized by the National Cybersecurity Centre, attended by the Crown Prince, His Royal Highness Prince Hussein bin Abdullah, with the more than 600 participants

Qatar - OCERT participated in the launch ceremony of educational cybersecurity curricula organized by the National Cybersecurity Agency

3 - 4 Oct 2023, Uzbekistan - OCERT participated in the Cybersecurity Conference

Participated in the Egypt Cybersecurity Conference and Exhibition with a panel discussion on current and emerging cybersecurity risks

OCERT organized the OIC-CERT Global Cybersecurity Award 2022

- **Regional Level**

Signing a cooperation framework for launching the Regional Cybersecurity Industry Environment Assessment Program for the Arab Region in collaboration with Huawei Middle East

The ITU-ARCC signed six MoU in the cybersecurity industry development and utilizing the services of the regional centre with:

- The Arab Organization for Information and Communication Technology
- The Arab Cybersecurity League
- The National Network Services Authority in the Syrian Arab Republic
- The Telecommunications Regulatory Authority in the Arab Republic of Egypt
- The Middle East Consultancy and Studies Center
- The Cybersecurity Council in the UAE
- The National Cybersecurity Centre in the Hashemite Kingdom of Jordan

Signing a memorandum of cooperation between the OIC-CERT and the Arab Organization for Information and Communication Technology

The Sultanate of Oman, represented by MTCIT, chaired the meeting of the Regional Working Group for the Arab Region of Study Group 17 on Telecommunication Standardization to introduce the cybersecurity industry program and present the innovation framework in cybersecurity

- **National Level**

Contributed to the implementation of electronic voting at the Ministry of Interior in the Sultanate of Oman

Trained 8 unemployed graduates to prepare them for employment

Activated secure connection between the government network and the networks of the Gulf Cooperation Council countries

Securely connected the government network with the cloud service providers Oracle, D2C & ODP

Provided 54 cybersecurity consultations for governmental institutions

Handled 770 change requests in the government network

Resolved 116 reported incidents of government network outages

Conducted security audits for 4 government entities as part of the information security compliance program

Participated in organizing technical workshops for the unified national portal project for government institutions

Secured 8 government sites, bringing the total number of secured sites to 128

Handled 35 change requests in server configurations for internet access

Conducted 8 security assessments for systems, websites, and networks of the MTCIT

Assessed the National Cyber Security Centre in Bahrain's application for FIRST membership

Issued over 3.6 million electronic certificates for various purposes

Issued 235 electronic signature tools for government and private sector employees

Completed the initial draft of the executive regulations for the Electronic Transactions and Digital Trust Law

The National Digital Forensic Laboratory achieved its eighth international recognition since 2016

Handled 241 digital evidence cases by the National Digital Forensic Laboratory, including 1430 digital pieces of evidence such as computers, mobile phones, and external storage devices

Handled 314 discovered and resolved security incidents

Issued 86 cybersecurity alerts and warnings related to security vulnerabilities, providing guidance for handling and resolving them

Organized the 9th national cybersecurity virtual exercise with the participation of various government institutions under the theme ‘Innovative Cyber Readiness to Counter Cyber Attacks and Risks’

Launched the national campaign for the cybersecurity industry '*Hadatha*' during the 10th media briefing of the MTCIT

Participated in the National Centre for Information Security in Sultan Qaboos University's professional exhibition, where the Hadatha program, aimed at localizing the cybersecurity industry and supporting innovation by empowering youth and enhancing their skills in the cybersecurity field was showcased

Participated in the National Centre for Information Security in the Third Omani Cybersecurity Forum at Sultan Qaboos University to promote the culture of the cybersecurity industry and raise awareness about advanced career opportunities

OCERT participated in a dialogue session within the National Information Security Week as part of the Hadatha national campaign

Signed a Memorandum of Cooperation between the MTCIT and the University of Technology and Applied Sciences to establish a Centre for Innovation and Excellence in Cybersecurity Industry (Hadatha Center) to enhance the cybersecurity industry in the Sultanate of Oman and provide an innovative cybersecurity environment for students

OCERT participated in hosting a visit from a delegation of the Gulf Cooperation Council countries in the field of information security

Keynote speech by the OCERT on '*Developing the Cybersecurity Industry*' during the German Conference on Safety and Cybersecurity

Conducted 2 workshops on the Hadatha Cybersecurity Industry Development Program and Innovation at the University of Technology and Applied Sciences in Muscat

Organized a panel discussion titled '*Career Path for Cybersecurity Professionals*' in collaboration with the Ministry of Labor and the Cyber Defence Centre

Conducted an awareness workshop on innovation and cybersecurity as a career path at Sultan Qaboos University

Conducted an awareness workshop on freelance work in the cybersecurity field in collaboration with the National Employment Program at the General Directorate for Stimulating the Sector and Future Skills

Participated in presenting a workshop on the Hadatha Cybersecurity Industry Development Program as part of the Cyber101 activities organized by the Small and Medium Enterprises Development Authority to enhance national capabilities

Participated in celebrating the World Internet Safer Day 2023

Executed and analysed studies and opinion polls to measure public familiarity with the Hadatha Cybersecurity Industry Development Program

Launched the National Centre for Information Security's new website identity during COMEX 2023 in line with the Hadatha Program

Supported and promoted the NTG Hacktivate competition in collaboration with NTG Company to enhance capabilities and refine skills in the cybersecurity field to meet the needs of the local market

Participated in COMEX 2023 exhibition

12 PAKISTAN

National Response Centre for Cyber Crimes – NR3C

12.1 ABOUT THE ORGANIZATION

12.1.1 Introduction

The National Response Centre for Cyber Crimes (**NR3C**) was established in 2007 as a Public Sector Development Programme (**PSDP**) funded Project

All officers and manpower of NR3C was regularized in 2012. All officers inducted in phase-II and phase-III of NR3C are in the process of regularization (to be permanent)

The Federal Investigation Agency Cyber Crime Wing (**FIA CCW**) is expected to expand its operational manpower and capacities at district level in coming years

12.1.2 Establishment

FIA CCW / NR3C is a state-run wing of the Federal Investigation Agency (**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. FIA CCW promotes the cybersecurity interests of the State of Pakistan at the national and international level through Rule of Law. FIA CCW/ NR3C is a full member of OIC-CERT since its first seminar in 2009 at Kuala Lumpur, Malaysia. Therefore, the objectives of FIA CCW/ NR3C are aligned with the objectives of OIC-CERT. Total manpower of FIA CCW/ NR3C comprises of 477 well trained staff

12.1.3 Resources

The public, national, and international

12.1.4 Constituency

National and international

12.2 HIGHLIGHTS OF 2023

12.2.1 Summary of Major Activities

Served as an active member of OIC-CERT

Online participation in OIC-CERT Trainings

11 - 13 Oct 2023 Abu Dhabi, UAE - 15th OIC-CERT Annual Conference. Delegates from FIA CCW

- *Syed Shahid Hassan*, Dir. Admin. FIA CCW
- *Muhammad Akram Mughal*, Deputy Director Network Security, FIA CCW
- *Zahid Bashir*, Asst. Dir. Investigation FIA CCW, physically participated in said session along with CERT Heads and Cyber Security Specialists from 57 OIC Member States and 12 observer states

*9 - 10 Oct 2023 Abu Dhabi U*AE - 11th Arab Regional, OIC-CERT & CIS Cyber Drill. Cybersecurity Specialist from FIA CCW:

- *Muhammad Akram Mughal*, Deputy Director of Network Security, FIA CCW
- *Zahid Bashir*, Asst. Dir. Investigation, FIA CCW,

  participated in said session along with Cybersecurity specialists from all 57 OIC member states and 12 observer states

Participation of FIA CCW Cyber Security Team in OIC-CERT & CIS Cyber Drill 2023 in Abu Dhabi, UAE

07-10 Nov 2023 Online - FIA CCW cybersecurity team lead by the Deputy Director of Network Security participated in the 3rd Africa Cyber Drill 2023 by the Mozambique National Computer Security Incident Response Team (CSIRT.Mz) and the Software Engineering Institute (**SEI**) of the Carnegie Mellon University, USA organized the 3rd edition of the Africa Cyber Drill in Radisson Blu Hotel Maputo, Mozambique

Organized cybersecurity, digital forensics and cyber laws seminars in universities/ academic institutes across Pakistan

FIA CCW Cybersecurity/ digital forensic experts were invited as guest speakers by various institutions of National prestige such as

- the Anti-Narcotics Force (**ANF**)
- Beaconhouse Margalla Campus Islamabad
- Securities and Exchange Commission (**SECP**)
- Islamabad Convent School H-8/4 Campus
- Froebels School F-7 Campus
- National University of Modern Language (**NUML**)
- FIA Academy (*for briefing to CSS officers*)

- National University of Sciences & Technology (**NUST**)
- National University of Medical Sciences (**NUMS**)
- FAST[5] National University Islamabad
- Overseas Pakistanis Foundation (**OPF**) Girls College F-8/2 Islamabad

FIA CCW officers contributed in identification process of CII

FIA CCW officers contributed to the Information Security Management System (ISO 27001) Audit of National Database and Registration Authority (**NADRA**) and Immigration and Passports (**IMPASS**)

Prevention of Electronic Crimes Act, 2016 was amended by the Cabinet to give powers to the police for registration of cybercrime complaints. Punjab Police alone is going to recruit 2000 cyber police officers in the coming few months

Deputy Director of Network Security FIA CCW supervised internship (40 days) of NUST MSIS Student

Deputy Director of Network Security supervised research work of two students from MS System Security, Air University on cyberbullying among children and motives of financial frauds through phishing respectively

[5] Foundation for Advancement of Science and Technology

12.2.2 Achievements

FIA CCW received more than 37,500 cybercrime complaints regarding financial frauds

FIA CCW received more than 8,660 cybercrime complaints regarding defamation

FIA CCW received more than 7,900 cybercrime complaints regarding harassment

FIA CCW received more than 6,340 cybercrime complaints regarding hacking

FIA CCW received more than 5,500 cybercrime complaints regarding blackmailing

12.3 ACTIVITIES & OPERATION

12.3.1 Events organized by the organization/ agency

The FIA Academy organized a briefing session for probationary officers of the 51st Common Training Programme (**CTP**). The Deputy Director of Network Security FIA CCW briefed said officers

12.3.2 Events involvement

FIA CCW officers officially attended the 15th OIC-CERT Annual Conference 2023

9 - 10 Oct 2023 Abu Dhabi, UAE - FIA CCW cybersecurity specialists lead by the Deputy Director Network Security FIA CCW, physically participated and contested in the 11th Arab Regional, OIC-CERT, & CIS Cyber Drill. This was

the world largest cyber drill base on the number of contestants/ participants

Delegates from Pakistan in OIC-CERT Annual Conference 2023 and OIC-CERT Cyber Drill 2023

The Deputy Director Network Security FIA CCW was invited by the Anti-Narcotics Academy as a guest speaker on cybersecurity, cybercrime laws and electronic evidence collection in narcotics cases

Beaconhouse Margalla Campus Islamabad, the largest campus of Beaconhouse in Pakistan, invited the Deputy Director Network Security FIA CCW to speak on cybersecurity

Figure 1xxx 5.5. Beaconhouse Margalla Campus Islamabad invited Dep Dir Network Security FIA CCW to deliver lecture on cybersecurity

SECP invited FIA CCW forensics officers Masood Ali – Incharge Forensics and Asma Majeed - Assistant Director Forensics to impart training on digital forensic investigation

Islamabad Convent School, H-8/4 Campus invited FIA CCW officers Sibtain Ahmed - Assistant Director Forensics, Asma Majeed - Assistant Director Forensics, Salman Riaz - Assistant Director Hardware, and Shahab Hussain - Assistant Director Accounts to conduct awareness session on cybercrimes

Islamabad Convent School, H-8/4 Campus invited FIA CCW officers to conduct awareness session on cybercrimes

Islamabad Froebels School F-7 Campus invited FIA CCW officers Sibtain Ahmed - Assistant Director Forensics, Asma Majeed - Assistant Director Forensics, Salman Riaz - Assistant Director Hardware, and Shahab Hussain -

Assistant Director Accounts to conduct awareness session on cybercrimes for O & A Level Students

Islamabad Froebels School, F-7 Campus invited FIA CCW officers to conduct awareness session on cybercrimes for O & A Level Students

NUML University Islamabad invited FIA CCW officers Sibtain Ahmed - Assistant Director Forensics and Asma Majeed - Assistant Director Forensics to conduct awareness session on cybercrimes for faculty and students

NUML Islamabad invited FIA CCW officers to conduct awareness session on cybercrimes for faculty and students

NUST University Islamabad Campus invited FIA CCW officers Rizwan Ahmed Assistant - Director Forensics and Asma Majeed - Assistant Director Forensics to conduct cyber awareness session for the faculty and students

NUST Islamabad Campus invited FIA CCW officers to conduct Cyber Awareness Session for Faculty and Students

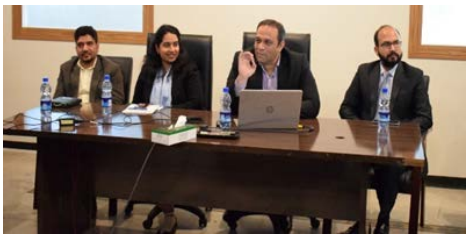
- OPF Girls College F-8/2 Islamabad invited FIA CCW officers to conduct cyber awareness sessions for the faculty and students

OPF Girls College F-8/2 Islamabad invited FIA CCW officers to conduct cyber awareness sessions for Faculty and Students

- NUMS University Rawalpindi invited FIA CCW officers to conduct cyber awareness session for the faculty and students

- FAST University Islamabad invited FIA CCW officers to conduct cyber awareness session for the faculty and students

NUMS University Rawalpindi invited FIA CCW officers to conduct cyber awareness session for faculty and students



FAST University Islamabad invited FIA CCW officers to conduct cyber awareness session for faculty and students

12.4 ACHIEVEMENTS

Establishment of 15 Forensic Labs across Pakistan

- Hiring of 406 new staff by CCW
- Conversion of 402 posts of CCW Phase-III project from Development to Non-development
- Revamping of CCW project
- Latest equipment procurement
- Establishment of 11 blasphemy units across the country
- Speedy relief to cybercrime complainant through the Helpdesk
- Establishment of specialized units to combat high-tech crimes

SECP invited FIA CCW officers to impart training on Digital Forensic Investigation

12.5 2024 PLANNED ACTIVITIES

Expansion of FIA CCW Division/ District Level

Human Resource Induction as per expansion Plan

Procurement of the latest digital forensics, network/ cybersecurity and cyber investigations

In-house development of Special Purpose Electronic Investigation Tools

Implementation of relevant ISO Standards in different sections of FIA CCW

Accreditation of the Digital Forensic Labs at Zonal Level from the Pakistan National Accreditation Council

Access of HEC Digital Library for FIA CCW officers to abreast them with the latest scientific and intellectual developments in the area of cybersecurity and digital forensics

Robust training plan for FIA CCW officers/ officials serving in labs and respective fields

15th OIC-CERT Annual Conference held on 11 to 13 October 2023 in Abu Dhabi, UAE, The 11th Arab Regional, OIC-CERT & CIS Cyber Drill held on 9th - 10th October 2023 in Abu Dhabi, UAE. Delegates from FIA Cyber Crime Wing Pakistan: 1- Syed Shahid Hassan, Dir. Admin, FIA CCW, 2- Muhammad Akram Mughal, Dy. Dir. Network Security, FIA CCW, 3- Zahid Bashir, AD Investigation ,FIA CCW in a Group Photo with CERT Heads and Cyber Security Specialists from All 57 OIC-CERT Muslim Countries and 12 Observer States

5 Guinness World World Record Broken and Registered: 1- Conference became largest Cybersecurity event of the World with over 70 nations participation 2- Cyber Drill recorded as largest ever cyber drill in the world with 162 cybersecurity specialists from over 70 nationalities 3- Event recorded as largest cybersecurity event in the world with respect to diversity of nations. 4- Biggest ever Simulation Modeling of Critical Information Infrastrcture in the world 5- Biggest ever Simulation Modeling of Cybersecurity Infrastrcture in the world

Pakistan Information Security Association – PISA

12.1 ABOUT THE ORGANIZATION

12.1.1 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 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 the professionals involved

12.1.2 Establishment

PISA was establishment in 2005

12.1.3 Resources

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

12.1.4 Constituency

Pakistan

12.2 HIGHLIGHTS OF 2023

12.2.1 Summary of Major Activities

26 Jul 2023 - The National Dialogue on the Role of CERT's

16 Aug 2023 - APCERT Cyber Drill 2023

Aug 2023 - National Cyber Drill for CSP

6 Sep 2023 Online - Cyber Competition

7 - 10 Nov 2023 - 3rd Africa Cyber Drill 2023

11 Nov 2023 - Conference on AI for Cybersecurity

Conference on Artificial Intelligence For Cybersecurity

13 Dec 2023 - Cyber Secure Pakistan (**CSP**)

Africa CERT Cyber Drill 2023

Pakistan Institute of International Affairs (**PIIA**) event AI for Cybersecurity

PISA conducted Cybersecurity Conference in Karachi in collaboration with PIIA

12.2.2 Achievements

In 2023 PISA has completed the following target

- *Aug 2023* - Participated in multiple significant cybersecurity events, including CSP Conference and the National Cyber Drill
- *6 Sep 2023* - Competed in the Online Cyber Competition on demonstrating practical cybersecurity skills
- *Nov 2023* - Engaged in international cyber preparedness through active involvement in the AfricaCERT Cyber Drill and the 3rd Africa CyberDrill

- *Nov 2023 - Contributed to the development and discussion of AI in cybersecurity at events such as the PIIA event and the Conference on AI for Cybersecurity*
- *Collaborated in organizing the PISA-conducted Cybersecurity Conference in Karachi, fostering local and international partnerships and dialogue*
- *Several students and professionals (universities & law enforcement) have been trained in cybersecurity and Information* Security by PISA

12.3 ACTIVITIES & OPERATION

12.3.1 Events organized by the organization/ agency

Tracking the Criminals in Cyber Space for Law Enforcement

Conference on Cyber Security in the 21st Century for Universities

Role of CERTs for Cybersecurity of National Assets for CERTs

12.3.2 Events involvement

Participated in CSP, Africa CERT Cyber Drill, and online cyber competitions

Engaged in PIIA events on AI for cybersecurity and conferences on AI for Cybersecurity

Attended the cybersecurity conferences conducted by PISA in Karachi and Africa Cyber Drill events

Joined the National Dialogue on the Role of CERT's and APCERT Cyber Drill.

Contributed to the National Cyber Drill for CSP and various other cybersecurity initiatives

12.4 ACHIEVEMENT

In 2023 PISA have achieved all targets set in 2022. Participated in the International Cyber Drills and successfully organized seminars and workshops. Provide services to law enforcement, public and private sector in the following

- *Guidelines* to minimize 'Threats of Ransomware'
- *Identification and responding to server-level threats*
- *Security assessments of different infrastructures*
- *Responding* to the cyber incident

12.5 2024 PLANNED ACTIVITIES

Planned to organize Cyber Secure Pakistan (CSP) International event.

Planned to organize the mega event on 'Cybersecurity on 21st Century'

Planned to organize in-house Cyber Security Drills

Planned to Participate in the International Cyber Security Drills, CTF competition, CyberLympics etc

Planned to organize Cybersecurity/ Information Security seminar, workshops for universities, government sector, and private sector

Online Cyber competition


PISA
CIT-CERT warmly welcomes you to
"The National Dialogue on the Role of CERTs"
OPPORTUNITIES AND WAY FORWARD
26 JULY 2023.


PANEL DISCUSSION
OIC-CERT Cybersecurity Industry Development
Dr. Haji Amirudin
Chief Executive Officer,
H.E Dr. Mohamed Hamad
Al Kuwaiti
Head of Cyber Security Council,
Mr. Tural Mammadov
Chief Information Security Officer,
Special Communication and Information
Security State Service of Azerbaijan
الأسبوع الإقليمي للأمن السيبراني ٢٠٢٢م
Regional Cybersecurity Week 2022

13 TUNISIA

National Agency for Computer Security – TunCERT

13.1 ABOUT THE ORGANIZATION

13.1.1 Introduction

The National Agency of Cyber Security is in charge and in coordination with the various parties involved in the field of supervising the security of the information and communication systems of the public and private structures of the national cyberspace

13.1.2 Establishment

According to the new legal framework, the National Agency of Cyber Security exerts mainly the following missions

Develop and update policies and mechanisms for the governance and security of the national cyberspace, and make them available to the relevant sectors and organizations

Monitor the implementation of action plans for the security of the national cyberspace concerning

- Proactive measures to avoid deliberate and accidental threats to the national cyberspace
- Preventive measures to protect against cyber risks
- Mechanisms for instant detection and reporting of cyber incidents and attacks
- Emergency response to cope with cyber-attacks and mitigate the impact
- Rapid recovery from the effects of cyber incidents and attacks to ensure business continuity
- Digital investigation to diagnose incidents and determine responsibility in relation to cybersecurity

Develop and monitor the implementation of skills development

programs in the field of cybersecurity through

- Participating in the development of specialized academic and professional programs in the field of cybersecurity
- Validating cybersecurity training programs and publishing them on the Agency's official website
- Organize specialized cybersecurity training sessions
- Develop and publish cybersecurity guidelines, models, and guides to be adopted by the public and private organizations
- Develop indicators to measure the national level of cybersecurity and publish dashboards periodically
- Implement periodic communication and awareness campaigns in the field of cybersecurity, particularly during cyber crises
- Maintain a technology watch and monitor developments in the field of cybersecurity
- International cooperation and coordination with foreign official structures in accordance with bilateral, regional and international agreements

13.1.3 Resources

The National Agency of Cyber Security departments are the following

- General Administration
- Conduct Control and Quality Management Unit
- Governance unit
- Unit according to the objectives to complete the project to focus on the information security management system
- Management of Information Emergency Response and Briefing
- Management of Information Systems Safety Technologies
- Information Security Audit Management
- Resource Management

13.1.4 Constituency

The national organizations

13.2 HIGHLIGHTS OF 2023

13.2.1 Summary of Major Activities

Updating the legal framework for cybersecurity and issuing the Decree Law No. 17 of March 11th, 2023

Cyber Incident Response

Organization of several awareness sessions

Cybersecurity Capacity Building

Support for implementing national projects related to cybersecurity

Provide immersion missions for the benefit of African and Arab CERTs

13.3 ACTIVITIES & OPERATION

13.3.1 Events organized by the organization/ agency

23 Nov 2023 - National Cyber Drill 2023

More than six (6) awareness sessions about the new legal framework for cybersecurity: Decree Law No. 17 of March 11th, 2023

More than five (5) awareness sessions about the best practices to secure systems and networks

13.3.2 Events involvement

12 Jan 2023 - Tunisie Telecom TT Security Day

04-05 Mar 2023 - Enterprises Days

19-21 Jul 2023 - Africa Crypt 2023 –.

16-17 May 2023 - Maghreb Cybersecurity & Cloud Expo- 2nd edition

30 Sep 2023 - Securiday

09-14 Oct 2023 Abu Dhabi, UAE - Regional Cybersecurity Week

05-06 Dec 2023 - Arab Cybersecurity Days/ AICTO

22-24 Dec 2023 - I-PROTECTv6

13.4 ACHIEVEMENTS

More than 6 awareness sessions about the new legal framework for cybersecurity: Decree Law No. 17 of March 11th, 2023

More than 5 awareness sessions about the best practices to secure systems and networks

12 Jan 2023 - Tunisie Telecom TT Security Day

04-05 Mar 2023 - Enterprise Days

16-17 May 2023 - Maghreb Cybersecurity & Cloud Expo- 2nd edition

19-21 Jul 2023 - Africa Crypt 2023

30 Sep 2023 - Securiday

09-14 Oct 2023 Abu Dhabi, UAE - Regional Cybersecurity Week

23 Nov 2023 - National Cyber Drill 2023

05-06 Dec 2023 - Arab Cybersecurity Days/AICTO

22-24 Dec 2023 - I-PROTECTv6

13.5 2024 PLANNED ACTIVITIES

Organize awareness sessions

Organization of events

Organization of cyber drills

Organization of immersion missions to tunCERT


الإطار القانوني للسلامة السيبرنية
بالجمهورية التونسية
ANCS


الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique


Dr. Yacine Djemail
Shaikh Abdulla Al Khalifa
H.E. Bassam Maharmeh
SECOND PANEL DISCUSSION
CYBERSECURITY:
STRATEGIC INSIGHTS


Regional Cybersecurity Week

14 TURKIYE

Turkcell CDC

14.1 ABOUT THE ORGANIZATION

14.1.1 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 a variety of services in the Information Security domain at national and international scale including threat intelligence, managed security operations centre, and DFIR services. Turkcell CDC also 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, the organization also has the following

- Distributed Denial of Service (**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

14.1.2 Establishment

Turkcell CDC is established on Dec 2015

14.2 HIGHLIGHTS OF 2023

14.2.1 Summary of Major Activities

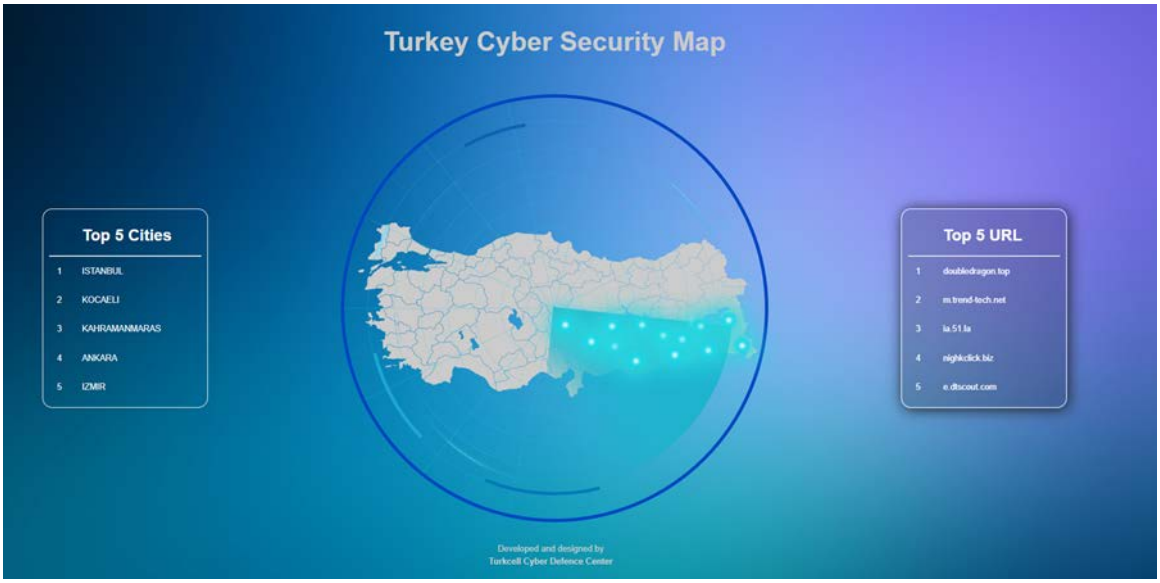
In 2023, Turkcell CDC continued to offer new cybersecurity services for the corporate and individual customers:

- **Threat Intelligence Service (Bozok)**

Turkcell CDC launched a threat intelligence platform called Bozok, which provides 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

Turkcell CDC Bozok Threat Intelligence Service



BOZOK TI infrastructure is powered by nearly 100 intelligence sources among them are

- CDC EYE
- dark web and threat intelligence forums
- Pastebin
- Github
- Twitter
- Virus Total

Detecting data leaks with automation and instant reporting, Bozok enables the customers to take early action. Such reports include threat actor reports specific to advanced APT groups and monitors ransomware groups detecting newly opened domains and warns customers against phishing attacks. The platform runs the take-down process for

detected fake domains and offers a 'Malware Analysis' interface to examine files that the customers suspect. Bozok provides information about existing vulnerabilities with the vulnerability centre. Stealer log notifies customers with malware integration. The number of customers had increased by 36% in 2023, as a result of the works carried out in this context

- **Turkcell Security Operation Centre Service**

Turkcell offers 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. The agency produce innovative ideas and develop quality products and services, and in this context, try to keep customer satisfaction at the highest level. Apart from the 24/7 monitoring service, there are various trainings provided by expert cybersecurity engineers to create cybersecurity awareness.

Turkcell 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 15% in 2023

- **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 adaptable 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 AI algorithms. The service informs the customers if they are using e-mail and social media accounts that have leaked passwords

-

Turkcell Cyber Defence Centre

Turkcell Security Orchestration, Automation and Response 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 in their fields and can respond to cyber incidents accurately and quickly using industry standard methodologies. In this context, Turkcell CDC launched Turkcell Security Orchestration, Automation and Response Service (**SOAR**) in 2021 for both Turkcell internal and SOC service customers to take faster and safer action for the engineers. As a result of the various studies and developments made, the number of customers increased by 35% in 2023 compared to 2022

- **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 in 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 a high level of knowledge, in more than 1,500 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

- **Cybersecurity 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:

- Cybersecurity 101 and Phishing
- Threat Intelligence
- SIEM Management
- Windows Forensic
- Malware Analysis

- **CDC Sense Honeypot**

The CDC Sense project enables to look at events from a larger perspective by tracking cyber-attacks around the world with more detail. This allows Turkcell first-hand attack information such as the command-and-control centre and malware used in attacks, and complete analysing of the attacker profiles. With this project, in which decoy systems located in 11 countries are developed, it enriches threat intelligence infrastructure and contribute to the increase in intelligence quality and raw data that are not shared in different intelligence networks are analysed gradually and added to the BOZOK Threat Intelligence infrastructure

14.2.2 Achievements

Turkcell CDC CTF teams participated in many CTF events in 2023 and ranked high. Some of these CTFs are: African Cyber Drill, APCERT 2023, STM CTF 2023

14.3 ACTIVITIES & OPERATION

14.3.1 Events organized by the organization/ agency

Turkcell attended the Take Off Istanbul 2023, the international startup summit, that brings together many entrepreneurs and mentors for innovation. The agency gave information on services and trainings to the visitors. There are also presentations on threat intelligence platform BOZOK, SOC Service, and Digital Security Service

Take Off İstanbul - 2023

14.3.2 Events Involvement

Turkcell CDC members made presentations and provided training on various cybersecurity issues at:

- Technology Talks
- Cyber Security Week
- Security Summit
- Take Off İstanbul 2023
- 16th International Conference on Information Security and Cryptology
- Turkey Cyber Security Cluster Week
- Information Security Association
- IDC Conferences

Turkcell CDC participated in the Take Off İstanbul 2023 and presented on various topics such as BOZOK Threat Intelligence and Digital Security Service

Within the scope of Turkcell's special recruitment program for young people, GNÇYTNK, the agency shared the Cybersecurity Approach at Turkcell to Young Talent friends who are interested in cybersecurity

GNCYTNK 2023 Meetings

14.4 ACHIEVEMENTS

Turkcell CDC CTF teams participated in many Capture the Flag events in 2023 and ranked high. Some of these CTFs are: African Cyber Drill, APCERT 2023, STM CTF 2023.

14.5 2024 PLANNED ACTIVITIES

Reaching more foreign customers by improving overseas customer work

Providing MDR service to the customers

Within the scope of the CDC Big Data Project, studies are carried out to ensure that long-term historical logs can be searched and examined quickly and easily in case of a possible cyber incident or during threat hunting studies

Use case development for product dissemination and detection of any suspicious activity within the scope of Identity Threat Detection and Response (**ITDR**) security project

15 UNITED ARAB EMIRATES

Cyber Security Council – aeCERT

15.1 ABOUT THE ORGANIZATION

15.1.1 Introduction

https://csc.gov.ae/

The UAE Cabinet granted approval in November 2020 for the establishment of the UAE Cybersecurity Council (**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 critical infrastructure 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 its digital transformation

15.1.2 Establishment

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

15.1.3 Resources

- **Services**

Policy and Strategy Development

- Developing national cybersecurity policies and strategies
- Conducting cybersecurity risk assessments and provide recommendations
- Providing guidance on regulatory compliance and best practices

Capacity Building and Training

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

Incident Response and Management

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

Research and Development

- 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 practice

- **Training and Education**

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

Cybersecurity Awareness Training

The council provides training and education to government agencies, private organizations, and the public on cybersecurity best practices and protection against cyber threats

Technical Training

The council provides technical training to government agencies and private organizations on how to use cybersecurity 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 cybersecurity regulations and standards

Cybercrime Investigations and Forensic Training

The council provides training to government agencies and private organizations on investigation and prosecution of cybercrime

Cybersecurity awareness campaigns

The council runs campaigns to educate the public about cybersecurity 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 cybersecurity and to encourage them to pursue cybersecurity-related careers

15.1.4 Constituency

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

15.2 HIGHLIGHTS OF 2023

15.2.1 Cyber Pulse Initiative

Cyber Drills

- The UAE CSC conducted a total of 12 cyber drills
- The cyber drills were attended by over 800 individuals
- The drills covered 200 distinct topics related to cybersecurity
- The drills were targeted at 90,000 federal and government entities

Future Leaders

- The UAE CSC conducted 52 cyber awareness sessions targeted at C-suite executives, directors, and managers
- The sessions were attended by 88,000 individuals, including high-level leaders from government and international entities
- The sessions covered 300 diverse topics related to cybersecurity
- The awareness sessions were specifically targeted at 900 federal and government entities to help them build their cybersecurity awareness and capabilities

15.2.2 Cyber Pulse for Society

The UAE CSC conducted 2,000 cyber awareness sessions

These sessions were attended by 100,000 people from various segments of the society, including families, senior citizens, and students

The sessions covered 500 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

15.2.3 Computer Emergency Response Services

11,604 cyber incidents have been dealt with

1928 sites were monitored against defacement

42,211,587 cyberattack attempts were confronted in 2023

Incorporating 18 new entities into a system based on the cybersecurity warning publications system

15.2.4 Cyber Security Awareness Services

67 awareness sessions provided.

3,409 people attended the awareness sessions

Cybersecurity Train-the-Trainer's sessions conducted for 32 trainers

15.2.5 Security Quality Services

1,776 vulnerabilities were discovered in systems and networks

70 penetration testing services provided

15.2.6 Cybersecurity Monitoring

17 entities on-boarded in Endpoint protection service

35 entities benefits from SIEM solutions

15.2.7 Compliance Services

Holding a specialized workshop on the standards of the national framework for ensuring Information security in UAE to educate representatives of federal

government entities about the standards, the implementation process, and the delivery of compliance reports

15.2.8 Collaborations with Global Partners

CSC signed MoUs with the following international partners to enhance cybersecurity strategies

- CPX
- Oracle
- Microsoft
- Hewlett Packard Enterprise
- Kela
- IBM
- SAP
- AWS
- IDC
- Huawei
- KPMG
- Madinat
- CyberArrow
- Immersive Labs
- Deloitte
- GBM
- Accenture
- Cisco
- Huawei

UAE CSC, AWS sign a MoU to accelerate cloud services adoption in UAE

MoU Signing between CSC and Huawei to strengthen local cybersecurity strategies

CSC collaborates with Etisalat, to improve its security posture and enhance the country's leading position in global competitiveness indicators

The signing of a MoU between the CSC and Splunk on the sidelines of GITEX Global 2023 Conference

H.E Dr. Al Kuwaiti signing a MoU between the CSC and @eccouncil

Etisalat signs a MOU with CSC

CSC signs a MOU with Advanced Technology Research Council

"مجلس الأمن السيبراني" يتعاون مع "مايكروسوفت"

وقّع مجلس الأمن السيبراني لحكومة دولة الإمارات وشركة مايكروسوفت مذكرة تفاهم بشأن التعاون في مجال الأمن السيبراني. وتحدد مذكرة التفاهم إطارًا للتعاون بين الطرفين من أجل إنشاء مجتمع معلومات آمن وعالمي. على هامش مؤتمر الأمن السيبراني في الشرق الأوسط، بحضور سعادة الدكتور محمد الكويتي رئيس الأمن السيبراني لحكومة دولة الإمارات ونعيم يزبك مدير عام مايكروسوفت الإمارات

توقيع مذكرة تفاهم للتعاون بين مجلس الأمن السيبراني وشركة أوراكل

تم التوقيع على مذكرة تفاهم بهدف توسيع التعاون في مجال الأمن السيبراني بين مجلس الأمن السيبراني وشركة اوراكل من جولة أوراكل كلاود العالمية في مركز أبوظبي الوطني للمعارض، بحضور سعادة الدكتور محمد الكويتي رئيس الأمن السيبراني لحكومة دولة الإمارات ونيك ريدشو نائب الرئيس الأول للتقنية السحابية في منطقة الشرق الأوسط وأفريقيا، ورئيس شركة أوراكل في دولة الإمارات.

15.2.9 Political Collaborations

The UAE CSC has established political collaborations with various organizations, to enhance the country's cybersecurity capabilities and promote international cooperation

- ITU
- Open-Ended Working Group (**OEWG**)
- Centre for Humanitarian Dialogue
- International Counter Ransomware Initiative (**CRI**)

1 Nov 2023 Washington DC, USA - the UAE 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 2023. The CRI was held under the auspices of the US White House and attended by US Vice President Kamala Harris

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

Riyadh, Saudi Arabia - the UAE CSC participated in the conclusion of the Global Cybersecurity Forum

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

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

The UAE 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

UAE CSC's participation in the P2C initiative help establish strong links with targeted countries and communities of this initiative such as the Least Developed Countries (**LDC**s), Landlocked Developing Countries (**LLDC**s) and Small Island Developing States (**SIDS**) and help strengthen UAE's position within the international multi-stakeholder alliances and support the overall eminence in the international cybersecurity landscape

Rwanda - The UAE CSC participated in the ITU World Telecommunication Development Conference (**WTDC**) to discuss future collaboration and mechanisms to enhancing cooperation on cybersecurity, including countering and combatting spam

15.2.10 Collaborations with National Entities

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

- Federal Authority for Government Human Resources
- Department of Energy - Abu Dhabi
- EDGE
- Cyber Gate
- Injazat
- Khalifa University
- CPX

The UAE CSC has joined the Ministry of Industry and Advanced Technology's National In-Country Value (**ICV**) Program

The UAE 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 UAE CSC and Abu Dhabi Department of Health aimed to raise awareness on 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

UAE 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

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

15.2.11 Achievements

Guinness World Record

The UAE CSC achieved 10 Guinness World Record

The UAE CSC achieved a Guinness World Record for hosting the largest number of attendees

The UAE CSC achieved a Guinness World Record for hosting the most users in a Cyber CTF video hangout

The UAE CSC achieved a Guinness World Record for hosting the largest bug bounty competition at the GISEC 2022

Global and International

Riyadh, Saudi Arabia - As a result of the UAE CSC's participation in the GCC Cybersecurity Ministerial Committee Meeting, the following achievements were made:

- Unified Gulf Cloud established to strengthen cybersecurity in the region
- Gulf Testing and Auditing Laboratory in development for enhanced cybersecurity
- Gulf Security Operations Centre adopted to bolster regional cyber defences
- New Anti-Ransomware Mechanisms formed in the Gulf Region to combat cyber threats

UAE CSC elected as Vice President 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 UAE 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 its partners to develop cutting-edge cybersecurity solutions and technologies. Through its 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

Passing the external audit of the ISO Certification in the Information Security Management System 27001

The aeCERT team won 3rd place in the OIC-CERT Award for Global Cybersecurity Response Teams 2023 for its Cybersecurity Warning Publications System

Managing and following up on the second phase of the National Information Security Framework project at the level of federal government agencies

15.3 ACTIVITIES & OPERATION

15.3.1 Events organized by the organization

The UAE CSC has organized several 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
- COP28
- Cyber Defense Day
- Global Media Congress
- Regional Cybersecurity Week

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

Organized a cybersecurity exercise '*Digital Shield*', with 4 realistic scenarios with 69 participants from 35 different entities

Hosted a workshop on '*Cyber Incident Response and Threat Intelligence*' and invited MSS, EDR, Sandbox, and threat experts. There were 25 participants from 16 different parties

15.3.2 Events involvement

The UAE 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
- Participated in a Cyber Drill organized by the OIC-CERT for response teams and obtained first place
- Participate within the technical committee for the 2023 national elections and provide advice and support in the field of cybersecurity for the website and the electronic application
- A delegation from the aeCERT team participated in the OIC-CERT meeting of response teams at Huawei's HQ in China

15.4 ACHIEVEMENTS

One of the notable achievements of the UAE 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
- Defence
- Nuclear

The significant achievements of the Cyber Pulse initiative successfully cover a wide range of society members, including:

- Youth Professional
- People of Determination
- Senior Citizen
- Workers

Members of the team were seconded as technical experts in several civil cases before the judicial authorities

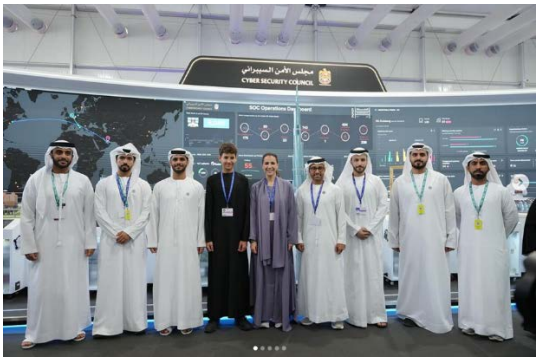
Eight (8) awareness sessions were delivered for the OIC-CERT and GCC in cooperation with strategic partners

32 government employees were trained on the awareness content developed for information security to be trainers

15.5 2024 PLANNED ACTIVITIES

The UAE 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 2024
- Safer Internet Day 2024
- IDEX 2024
- IDC CIO 2024
- World Police Summit 2024
- InterSec 2024
- GISEC 2024
- GITEX 2024
- GITEX Africa 2024


مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
المؤتمر الصحفي
للاحتفال باليوم العالمي
للانترنت الآمن 2024
كن آمناً رقمياً
معاً من أجل إنترنت أفضل


مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
NSRC


مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
#الانترنت_أفضل_استخداماً_في_الإمارات


WORLD ECONOMIC FORUM
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


SOC Operations
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


Gold Sponsors
METRON AVIATION
RTX
FlightAware
ADB SAFEGATE
Silver Sponsors
serco
FREQUENTIS
Supported by
dans
DUBAI AIRSHOW
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


WORLD ECONOMIC FORUM
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


المؤتمر رفيع المستوى لمكافحة الإرهاب
التصدي للإرهاب من خلال تنشيط التعددية والتعاون المؤسسي
من 19 إلى 23 يونيو 2023
مقر الأمم المتحدة - نيويورك
أهداف المؤتمر:
توفير منصة لتبادل المعلومات والخبرات والممارسات الجيدة
استكشاف مزيد من التعاون بشأن الأولويات الرئيسية لمكافحة الإرهاب
41 حدثاً جانبياً بالاشتراك بين الدول الأعضاء وكيانات الاتفاق العالمي لمكافحة الإرهاب :
تبادل الآراء حول الأولويات الرئيسية وكذلك تنفيذ الركائز الأربع لاستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب
توفير منصة لجمع المسؤولين رفيعي المستوى والخبراء لمشاركة أفضل ممارساتهم وتعزيز الجهود المشتركة
@cscgovae
Cyber Security Council | مجلس الأمن السيبراني


GLOBAL MEDIA CONGRESS
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


AMCHAM
ABU DHABI
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


GLOBAL MEDIA CONGRESS
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


Regional Cybersecurity Week
الأسبوع الإقليمي للأمن السيبراني
أبو ظبي / 2023
ITU


مجلس الأمن السيبراني
CYBER SECURITY COUNCIL


GITEX
AFRICA
Morocco
31 MAY
02 JUNE 2023
MARRAKECH
CAPTURE THE FLAG
LARGEST CYBER EXERCISE IN AFRICA
REGISTRATION OPENS
GITEX CYBER WARGAMES DAY 2
WINNERS ANNOUNCEMENT
22 MAY
31 MAY
1 JUNE
2 JUNE
2 JUNE
GITEX CYBER WARGAMES DAY 1
GITEX CYBER WARGAMES DAY 3


Shaping the Future of Cybersecurity in an Era of Complex Information Challenges

16 YEMEN

Smart Security Solutions Company - SMARTSEC

16.1 ABOUT THE ORGANIZATION

16.1.1 Introduction

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

16.1.2 Establishment

Dr. Abdulraman Muthana and a group of Information security professionals establish SMARTSEC in Oct 2010

16.1.3 Resources

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

16.1.4 Constituency

Information Security fields

16.2 HIGHLIGHTS OF 2023

16.2.1 Summary of Major Activities

Ethical Hacking and Penetration Testing training for cybersecurity professionals

Network, web, and mobile App penetration testing for a number of financial enterprises

Establishment of information security programs for a number of governmental agencies

Ransomware Analysis for a software development company

Fraud Investigations in some local banks

ISO 27001 training for a number of cybersecurity professionals

16.2.2 Achievements

Establishment of special cybersecurity courses for non-IT staff

Implementing Data Leak Prevention (**DLP**) solutions for some organizations

Investment on AI research in cybersecurity

Investment on Anti Ransomware development

16.3 ACTIVITIES & OPERATION

16.3.1 Events organized by the organization/ agency

Cybersecurity awareness training for banks employees

Seminars on AI and cybersecurity

Cybersecurity training for certification preparation

16.3.2 Events involvement

Implementing information security programs for several governmental agencies

Development of security policies for higher education

Training of ISO 27000 courses

Performing fraud investigations for some local financial companies

16.4 ACHIEVEMENT

Training a few advanced cybersecurity courses

Implementing DLP solutions

Investigating Ransomware virus incidents

16.5 2024 PLANNED ACTIVITIES

The company aims to continue investment in AI cybersecurity research in and development of Anti Ransomware solutions

More engagement in helping organizations in Yemen to implement ISO 27000 - ISMS Standard

17 NON OIC COUNTRY

CERT-GIB - Group-IB

17.1 ABOUT THE ORGANIZATION

17.1.1 Introduction

CERT-GIB is the CERT created by the global cybersecurity company Group-IB. It is launched with the mission to immediately contain cyber threats, regardless of when they happen, where they take place, and who were 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 member, CERT-GIB is a member of the Trusted Introducer, Anti-Phishing Working Group (**APWG**), FIRST, APCERT, Europol European Cybercrime Centre's (**EC3**) Advisory Group on Internet Security, and a strategic partner of Afripol

17.1.2 Establishment

CERT-GIB was established on 10 Mar 2011

17.1.3 Resources

Digital Crime Resistance Centres

Group-IB has a global presence in 60 countries with 5 Unique Digital Crime Resistance Centres (**DCRC**) in the Asia-Pacific, Middle East and Africa, Europe, and Central Asia, and this network is set to expand further over the coming years

DCRCs operate independently from one another and are staffed with highly experienced researchers who are tasked with investigating cyber-crimes, responding to incidents, monitoring local threats, and assessing regional trends to support its client base and growing partner network

More than 50 analysts of CERT-GIB are also part of the DCRCs. It allows CERT-GIB to analyse local threat landscapes, predict cyber risks, promptly respond to threats, and share continuously adversary-centric intelligence with other regions

Within the DCRCs, CERT-GIB works closely with other Group-IB's teams, including Digital Risk Protection, Digital Forensics Laboratory, Fraud Protection, Attack Surface Management, Threat Intelligence & Attribution, and Investigations

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 and Digital Risk Protection platforms

Combined, Group-IB technological capabilities include:

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

Expertise

Group-IB has provided more than 1,300 successful investigations and has spent over 70,000 hours responding to incidents of various complexity all over the globe. Group-IB has conducted extensive research on APT groups, ransomware operators, and general cybersecurity trends across all major industries. Group-IB's combined technological capabilities and human intelligence means the company is always aware of cyber criminals' latest tools, Tactics techniques and procedures (**TTP**s), and movements. CERT-GIB is an integral part of these activities

17.1.4 Constituency

CERT-GIB provides its services to protect more than 400 corporate brands. It also cooperates with government organizations and law enforcement agencies on issues related to cyber-attacks and protecting Internet users from cyber-crimes.

17.2 HIGHLIGHTS OF 2023

17.2.1 Summary

The number of phishing and scam resources detected by CERT-GIB increased by 3% and 8% percent, respectively

CERT-GIB responded to 114,637 phishing resources and 343,379 scam resources. 99% of violations were successfully solved

Group-IB took part in a global INTERPOL-led law enforcement operation named Synergia, aimed at combating the surge of phishing, banking malware, and ransomware attacks in more than 50 countries, and in the cross-border cyber-crime fighting operation Digital Skimming Action, coordinated by Europol and featuring the European Union Agency for Cybersecurity (**ENISA**), law enforcement authorities from 17 countries, and other private sector partners

Organized 6 events and training and participated in 42 industry & third-party events

Released two comprehensive annual reports on threat landscapes and more than 20 other analytical and technical reports

Group-IB's flagship Unified Risk Platform (**URP**) has been revamped to improve threat detection efficacy, enhance intelligence gathering, and fortify AI capabilities across its modules

17.2.2 Awards

Singapore Police Force Alliance of Public Private Cybercrime Stakeholders (**APPACT**) Appreciation Award 2023

6th Regulation Asia Awards for Excellence 2023: Anti-Fraud Project of the Year

Recognized by Gartner in the 2023 Market Guide for Digital Forensics and Incident Response Services as a representative vendor for incident response services

Frost & Sullivan's 2023 Competitive Strategy Leadership Award

Frost & Sullivan recognized Fraud Protection as the most complete anti-fraud solution currently on the market

Group-IB's Anastasia Tikhonova, Jennifer Soh, and Vesta Matveeva named among Top 30 Women in Security ASEAN Region 2023

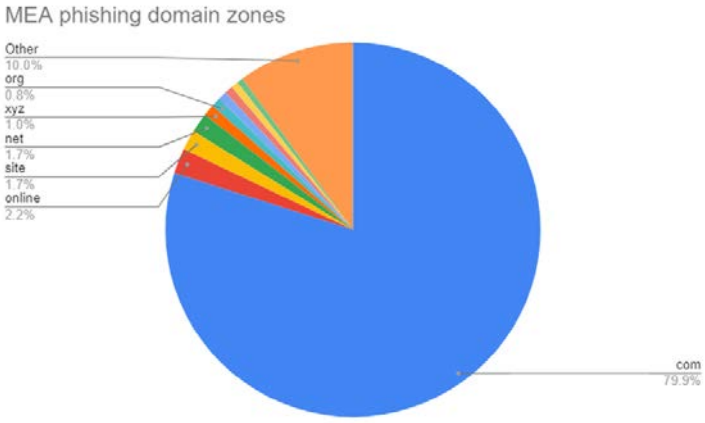
2023 Benelux Outstanding Security Performance Award (**OSPA**) for Outstanding Police/Law Enforcement Initiative

17.3 ACTIVITIES & OPERATION

17.3.1 Anti-Phishing and Anti-Scam statistics

In 2023, the number of phishing and scam resources detected by CERT-GIB increased by 3% and 8% percent, respectively

Among the Top Level Domains (**TLD**s) where criminals preferred to register phishing domains which attacks countries in the Middle East and Africa (**MEA**) region, the top 5 were .com (79,9%), .online (2,2%), .site (1,7%), .net (1,7%), .xyz (1,0%)



One of the key responsibilities of CERT-GIB is not only to detect violations, but also to take down violating resources. CERT-GIB actively interacts with domain name registrars, TLD administrators, ISPs, as well as with other CERT and CSIRT teams to eliminate the violations

In 2023, CERT-GIB responded to 114,637 phishing resources and 343,379 scam resources. 99% of violations were successfully solved

17.3.2 Special Operations

Group-IB took part in a global INTERPOL-led law enforcement operation named Synergia, aimed at combating the surge of phishing, banking malware, and ransomware attacks in more than 50 countries. As part of the global operation, the Group-IB team identified more than 500 IP addresses hosting phishing resources and over 1,900 IP addresses associated with ransomware, trojans, and banking malware operations. This information was then shared with the task force for

further coordinated action. The operation, which ran from Sep to Nov 2023, resulted in the apprehension of 31 individuals, the identification of an additional 70 suspects, and the takedown of hundreds of command-and-control servers.

Group-IB took part in the cross-border cybercrime fighting operation Digital Skimming Action, coordinated by Europol and featuring ENISA, law enforcement authorities from 17 countries, and other private sector partners. This helped Europol and partners to detect and issue notifications to 443 online merchants in total with whom customers' credit or payment card data had been potentially stolen

17.3.3 Events and trainings organized by the organization

Pakistan - Group-IB Threat Intel

Webinar - DRP: '*Safeguarding African Banks'*

Webinar: '*Mastering Attack Surface Management for Resilient cyber defence'*

Tanzania – '*Uncovering the unknown: Group-IB's Proactive Cyber Threat Defence'*

Fraud Day (French) for Côte D'Ivoire clients

Respond Like A Rockstar' DFIR Webinar

20th Anniversary CTF

Additionally, Group-IB has special training programs for commercial customers and government organizations which include

- Complex 4-months training on cybersecurity for SOC analysts
- Threat Intelligence Analyst
- Threat Hunter
- Windows DFIR Analyst
- Anti-Fraud Analyst

17.3.4 Industry and 3rd party events involvement

Ashraf Koheil, Group-IB's Regional Sales Director META (left), Jalel Chelba, Ag Executive Director of AFRIPOL (middle) and Group-IB CEO Dmitry Volkov (right)

Pacific Tech Singapore Product Launch 2023

Pacific Tech Indonesia Solutions Day 2023

Ngee Ann Polytechnic's Industry Partners Appreciation

Malaysia - VMware Security Connect

Kuala Lumpur, Malaysia - Pacific Tech '*Defence of the Era*'

ATxSG (Asia Tech & Singapore) 2023

Singapore - INTERPOL Global Cybercrime Conference 2023

Cyber Security Agency (CSA) Innovation Day 2023

Sarawak, Malaysia - WCIT 2023

INTERPOL Global Cybercrime Conference 2023

Singapore - GovWare 2023

Singapore - Merchant Risk Council

Employee Provident Fund (**EPF**) Cybersecurity Day 2023

SPF International Economic Crime Course (IECC) 2023

Abu Dhabi, UAE - The Dark Side of Finance

South Africa - IDC CIO Summit,

Egypt - CAISEC,

TFG Partner Universe

MENA ISC

Dot Cyber Summit

Partner Universe with TFG

Tanzania Roundtable Event

Jordan - Dot Cyber Summit,

EDEX Egypt

GITEX 2023

Secure 360 Event - MCS

UAE - GEC Media Award *Saudi Arabia* - Black Hat

Qatar - CYSEC

Gartner SRM Summit

Saudi Arabia - Suhoor Event

Egypt - Suhoor Event

Kuwait - Suhoor Event

Jordan - Suhoor Event

17.3.5 Publications

In 2023, Group-IB actively participated in cyber threat research, including studies of new phishing and scam schemes, malware and ransomware, APT groups and their attack vectors. The results of these studies were presented in the form of analytical and technical reports, press releases, blogs and other publications

Two (2) comprehensive annual reports were released

- *Hi-Tech Crime Trends 2022/2023* illustrating the actual threat landscape, specifying valuable data and sharing major insights
- *Digital Risk Trends 2023* provides a detailed analysis of trends in scams and phishing across different industries and regions

Threat reports that have generated significant industry interest include

- *W3LL done* - uncovering hidden phishing ecosystem driving BEC attacks
- *Beyond OWASP Top 10* - The ultimate guide to web application security (2023 and onwards)
- *Old Snake, New Skin* - Analysis of SideWinder APT activity in 2021

- *Ace in the Hole* - exposing GambleForce, an SQL injection gang
- *Curse of the Krasue - New Linux Remote Access Trojan targets Thailand*
- *Ransomware manager - Investigation into 'farnetwork', a threat actor linked to five strains of ransomware*
- *Let's dig deeper - dissecting the new Android Trojan 'GoldDigger' with Group-IB Fraud Matrix*
- *Dusting for fingerprints – 'ShadowSyndicate', a new RaaS player*
- *From Rags to Riches: The illusion of quick wealth in investment scams*
- *Stealing the extra mile - How fraudsters target global airlines in air miles and customer service scams*
- *New hierarchy, heightened threat – 'Classiscam's' sustained global campaign*
- *Traders' Dollars in Danger - CVE-2023-38831 zero-Day vulnerability in WinRAR exploited by cybercriminals to target traders*
- *Breaking down 'Gigabud' - banking malware with Group-IB Fraud Matrix*
- *Demystifying Mysterious Team Bangladesh*
- *Busting 'CryptosLabs' - a scam ring targeting Frenc*h speakers for millions
- *Dark Pink* - Episode 2
- *Dark Pink*
- *The distinctive rattle of APT SideWinder*
- *You've been kept in the dark (web)* - exposing Qilin's RaaS program
- *Tech (non)support - Scammers pose as Meta in Facebook account grab ploy*
- *Investigation into 'PostalFurious' - a Chinese-speaking phishing gang targeting Singapore and Australia*
- *'SimpleHarm' - tracking 'MuddyWater's' infrastructure*
- *The old way: 'BabLock', new ransomware quietly cruising around Europe, Middle East, and Asia*
- *36gate - supply chain attack*
- *Venomous vacancies - Job seekers across MEA hit by sting in scammers' tail*
- *Bleak outlook - Mitigating CVE-2023-23397*
- *Package deal - Malware bundles causing* disruption and damage across EMEA
- *Nice Try Tonto Team*

17.3.6 Technology

Group-IB's flagship URP has been revamped to improve threat detection efficacy, enhance intelligence gathering, and fortify AI capabilities across its modules

Fraud Protection module has been upgraded with a whole new Fraud Matrix framework. Based on the MITRE ATT&CK® model, Group-IB's Fraud Matrix allows users to deconstruct and catalogue fraud schemes, regardless of their complexity and number of stages, to better understand TTPs leveraged by fraudsters. Precise fraud categorization is achieved through the enrichment of

another brand-new feature, Fraud Intelligence.

Digital Risk Protection module has been empowered with AI algorithms to improve the detection efficiency of phishing and scam websites that impersonate legitimate companies. An enhanced AI-infused engine helps in the automated creation of signatures to speed up the detection of typo squatting and illicit use of brand logos. The implementation of the large-scale computer vision system has improved the detection rate of unauthorized brand logo usage by 40%, while, at the same time, implementing a three-fold decrease in the neural network's training time

Smart Abuse Tool has been released. It is a managed takedown assistant that enables CERT-GIB analysts, customers and managed security service providers (**MSSP**) partners to eliminate IP violations seamlessly and independently

Threat Intelligence module has been supercharged to improve the efficiency of the company's patented Graph Network Analysis tool. Group-IB has further expanded its intelligence-gathering network by implementing real-time cybersecurity news monitoring and IOCs filtering and extraction capability. The module now offers extended coverage of scanning hosts, VPN hosts, DDoS, and augmented phishing attacks

The Managed Extended Detection & Response (**MXDR**) has been extended its functionality to Linux and MacOS systems as well as remediation functionality for Windows EDR. Malware detonation has undergone a series of AI-driven optimizations to enhance the detection of "malware-free" attacks

Attack Surface Management's capabilities has been extended to cover typo squatting detection. Another new feature is the introduction of Group-IB's live Telegram bot for notification alerts and remediation guidance

17.3.7 Collaborations

Extended strategic partnership with the INTERPOL

Became a member of the newly formed Cyber Security Action Task Force (**CSATF**), led by the Hong Kong Police Force. The task force marks the significant collaboration between prominent cybersecurity companies,

Signing of the MoU by Head of Cyber Security for the UAE Government His Excellency Dr. Mohammed Hamad Al Kuwaiti and Ashraf Koheil, Regional Sales Director META at Group-IB

public service providers, and law enforcement agencies to strengthen the exchange of critical cyber threat intelligence, to prevent attacks in the early stages, and to facilitate the investigations of digital crimes

Signed a MoU with AFRIPOL. Group-IB will share its technological advancements and specialized knowledge in cyber investigations, reverse engineering, and incident management with AFRIPOL's personnel throughout the African member states, as the organization intensifies its efforts to address cybercrime continent-wide

Signed a MoU with the UAE CSC

Signed a MoU with the Defence Technology Institute (**DTI**), a government agency under the supervision of the Minister of Defence of Thailand

Signed a strategic partnership with CORVIT, the premiere source of IT and business knowledge and training in the UAE and surrounding areas

17.4 2024 PLANNED ACTIVITIES

17.4.1 Future Plans

Opening of Digital Crime Resistance Centres in new regions and countries

Strengthening CERT-GIB through deepening cooperation with the Threat Intelligence team

Further improvement and implementation of AI-based solutions in detection, automated collection of evidence, as well as response

Establishing new partnerships with government and law enforcement agencies in different countries

17.5 FUTURE EVENTS

OT-ISAC TTX

Singapore - Seamless Asia 2024

Jakarta, Indonesia - Pacific Tech Solutions Day 2024

Singapore Fraud Protection C-Level Roundtable

CyberSec Malaysia

Singapore - Regulation Asia Fraud & Financial Crime Event 2024

Jakarta, Indonesia - IndoSec 2024

Partner Universe

Singapore - GovWare 2024

UAE - GISEC 2024

UAE - IDC CISO Roundtable

Morocco, - GITEX 2024

UAE - Partner Universe MEA

Saudi Arabia - Partner Universe KSA

Jordan - Dot Cyber Summit

Turkey - IDC Security Summit

BlackHat, Saudi Arabia

UAE - World Police Summit

UAE - Gartner SRM Summit

CYSEC Qatar

Fraud Intel Series - KSA, UAE, Qatar, Pakistan, Kuwait, Bahrain

Group-IB's Head of Business Development (APAC) Wei See Wong receives the Anti-fraud Project of the Year award

Group-IB's Head of Business Development (APAC) Wei See Wong receives Singapore Police Force Alliance of Public Private Cybercrime Stakeholders (APPACT) Appreciation Award 2023

Acronyms

A

ABA - Azerbaijan Banks Association
ACCT - Arab Cybersecurity Cooperation Team
ACOA - Association of Cybersecurity Organizations of Azerbaijan
ACSRT - African Center for the Study and Research on Terrorism
ADEX – Azerbaijan Defence Exhibition
ADPU - Azerbaijan State Pedagogical University
AICTO - Arab Information & Communication Technologies Organization
AI – Artificial Intelligent
AITI - Authority for Info-communications Technology Industry
AJCCBC - ASEAN Japan Cybersecurity Capacity Building Centre
ANF - Anti Narcotics Force
APBn - Armed Police Battalion
APCERT – Asia Pacific Computer Emergency Response Team
APPACT - Singapore Police Force Alliance of Public Private Cybercrime Stakeholders
APT - Advance Persistence Threats
APWG - Anti-Phishing Working Group
ARCC - Arab Regional Cybersecurity Center
AUCSEG -
African Union Cybersecurity Expert Group
AZERTAC - Azerbaijan State News Agency
AzTU - Azerbaijan Technical University

B

BCSA - Brunei Cyber Security Association
BDSAF - Bangladesh System Administrators Forum
BDT - ITU Telecommunication Development Bureau
BOI - Bank of Industry

C

CBJ - Central Bank of Jordan
CCA - Controller Of Certifying Authorities
CID -Criminal Investigation Department
CIDC - Critical Infrastructure Defence Challenge
CII – Critical Information Infrastructure
CISA - Cybersecurity & Infrastructure Security Agency
CISO – Chief Information Security Officer
CPN - Computer Professional of Nigeria
CPrN - Computer Professionals Registration Council
CRDF - Civilian Research and Development Foundation Global
CRI – International Counter Ransomware Initiative
CSATF - Cyber Security Action Task Force
CSC – Cyber Security Center
CSC – Cyber Security Council (UAE)
CSB - Cyber Security Brunei
CSEAN - Cyber Security EXPERTS association of Nigeria
CSIRT - Computer Security Incident Response Team
CSIS - Center for Strategic and International Studies
CSP - Cyber Secure Pakistan
CTF – Capture the Flag
CTI – Computer Telephony Integration

CTP - Common Training Programme
CWC - Cyber Watch Centre

D

DCRC - Digital Crime Resistance Centre
DDoS - Distributed Denial of Service
DFIR - Digital Forensics and Incident Response
DLP - Data Leak Prevention
DNS - Domain Name System
DTI – Defence Technology Institute

E

EC3 - Europol European Cybercrime Centre
EDGE - Enhancing Digital Government & Economy
EDR - End point Detection Response
EGNC - E-Government National Centre
ENISA - European Union Agency for Cybersecurity
ENEC - Emirates Nuclear Energy Corporation
EPF - Employee Provident Fund
ERP - Executive Registration Programme
ESCWA - United Nations Economic and Social Commission for Western Asia

F

FIA CCW - The Federal Investigation Agency Cyber Crime Wing
FIRST - Forum for Incident Response Team

G

GCA - Global Cybersecurity Agenda
GC3B - Global Conference on Cyber Capacity Building
GCCD - Global Cybersecurity Center for Development
GCMC - George C. Marshall European Center for Security Studies
GCSC - Global Commission on the Stability of Cyberspace
GFCE - Global Forum on Cyber Expertise
GISEC – Gulf Information Security Expo & Conference
GUI - Graphical User Interface

H

HEI - Higher Education Institution
HND - Higher National Diploma

I

ICANN - Internet Corporation for Assigned Names and Numbers
ICS - Industrial Control System
ICV – In-Country Value
ID4D - Digital Identification for Development
IDEA - Innovation Design and Entrepreneurship Academy
ILCICT - International Libyan Conference on Information and Communications Technology
ILEA - International Law Enforcement Academy
IMPASS - Immigration and Passports
IOC - Indicator of Compromise
iOCTA - Internet Organised Crime Threat Assessment
IOT – Internet of Things
ITDR - Identity Threat Detection and Response
ITPSS - Information Technology Protective Security Services
ITU - International Telecommunication Union
ITU-GCI – ITU Global Cybersecurity Index

ITU-RCC - ITU Arab Regional Cyber Security Center
ISP – Internet Service Provider
IVLP - International Visitor Leadership Program

K

KISA - Korea Internet Security Agency
KOICA - Korea International Cooperation Agency

L

LDC - Least Developed Country
LEA – Law Enforcement Agency
LLDC - Landlocked Developing Country
LMS – Learning Management System

M

MEA - Middle East and Africa
MIST - Military Institute of Science and Technology
MoU - Memorandum of Understanding
MSSP - Managed Security Service Providers
MTCIT - Ministry of Transport, Communications and Information Technology
MTIC - Ministry of Transport and Infocommunications
MXDR - Managed Extended Detection & Response

N

NAP - Network Access Provider
NADRA - National Database and Registration Authority
NBTE - National Board for Technical Education
NCAA - Nigeria Civil Aviation Authority
NCCIS - National Coordination Centre for Information Security
NCS - Nigeria Computer Society
NDA - Non-Disclosure Agreement
NGFW - next-generation firewall
NIMS - National Digital Identity Management Systems
NUML - National University of Modern Language

O

OEWG - Open-Ended Working Group
OSCE - Organization for Security and Co-operation in Europe
OSPA - Outstanding Security Performance Award
OPF - Overseas Pakistanis Foundation

P

PIIA - Pakistan Institute of International Affairs
PKI - Public Key Infrastructure
PKSF - Palli Karma-Sahayak Foundation
PSDP - Public Sector Development Programme

R

RBPF - Royal Brunei Police Force
RDF-ARB - Regional Development Forum for Arab States

S

SECP - Securities and Exchange Commission
SEI - Software Engineering Institute
SIDS - Small Island Developing State
SIEM - Security Information and Event Management
SMB – Server Message Block

SOAR - Security Orchestration, Automation and Response
SOC - Security Operation Centre
SSH - Secure Shell Connection

T

TAG - Talal Abu Ghazaleh International Group
TF-CSIRT - Trusted Community CSIRT
TI-CSIRT - Trusted Introducer CSIRT
TLD – Top Level Domain
TTP - Tactics techniques and procedures

U

UN – United Nations
UNDOC – United Nations Office on Drugs and Crime
UNN - Unified National Network
URP - Unified Risk Platform

V

VAPT - Vulnerability assessment and penetration testing

W

WG – Working Group
WTDC - ITU World Telecommunication Development Conference

X

XRITDX - Special Communication and Information Security of the Republic of Azerbaijan