OIC-CERT 2020

ANNUAL REPORT

Organization of the Islamic Cooperation
Computer Emergency Response Team

ABOUT THE OIC-CERT

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

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

VISION

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

MISSION

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

OBJECTIVES

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

Encouraging the sharing of cybersecurity experience and information.

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

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

Promoting collaborative research, development, and innovation in cybersecurity

Promoting international cooperation with international cybersecurity organizations.

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

MEMBERSHIPS

BOARD MEMBERS 2020

Oman *(Chair)*
Oman National Computer Emergency Response Team (OCERT)

Malaysia *(Permanent Secretariat)*
CyberSecurity Malaysia

Azerbaijan
Azerbaijan Government CERT (CERT.GOV.AZ)

Egypt
Egypt Computer Emergency Response Team (EG-CERT)

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

Iran
Iran Computer Emergency Response Team (IRCERT)

United Arab Emirates
UAE Computer Emergency Response Team (aeCERT)

FULL & GENERAL MEMBERS

Azerbaijan
Azerbaijan Government CERT (CERT.GOV.AZ)

Bangladesh
- Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)
- *BangladeshCERT*
- *Bangladesh Computer Emergency Response Team (bdCERT)*

Brunei Darussalam
Brunei Computer Emergency Response Team (BruCERT)

Cote D'Ivoire
Cote D'Ivoire Computer Emergency Response Team (CI-CERT)

Egypt
Egypt Computer Emergency Response Team (EG-CERT)

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

Iran
- Iran Computer Emergency Response Team (IRCERT)
- *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)*

Jordan
Jordan Computer Emergency Response Team (JO-CERT)

Kazakhstan
- Kazakhstan Computer Emergency Response Team (KZ-CERT)
- *Center for Analysis and Investigation of Cyber-Attacks (CA ICA)*

Kuwait
Kuwait National Cyber Security Centre (NCSC-KW)

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

Libya
Libyan Computer Emergency Response Team (Libya-CERT)

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

Morocco
Moroccan Computer Emergency Response Team (maCERT)

Nigeria
Consultancy Support Service Limited (CS2)

Oman
Oman National Computer Emergency Response Team (OCERT)

Pakistan
- Pakistan Information Security Association (PISA-CERT
- *National Response Centre for Cyber Crimes (NR3C)*

Qatar
Qatar Computer Emergency Response Team (Q-CERT)

Saudi Arabia
Saudi Arabia Computer Emergency Response Team (CERT-SA)

Somalia
Somalia Computer Emergency Response Team (SomCERT)

Sudan
Sudan Computer Emergency Response Team (SudanCERT)

Syria
National Agency for Network Services

Tunisia
National Agency for Computer Security (tunCERT)

Turkey
National Cyber Security Incident Response Team (TR-CERT)

Uganda
Uganda Computer Emergency Response Team (UG-CERT)

United Arab Emirates
UAE Computer Emergency Response Team (aeCERT)

Uzbekistan
Uzbekistan Computer Emergency Response Team (UzCERT)

AFFILIATE MEMBER

Team Cymru, USA

COMMERCIAL MEMBERS

CERT-GIB, Singapore

Duzon, South Korea

Huawei, UAE

Insight Security Operation Centre, Oman

Serba Dinamik Group Berhad, Malaysia

Turkcell Cyber Defence Centre, Turkey

PROFESSIONAL MEMBERS

Abdul Fattah Mohamed Yatim - Teknimuda (M) Sdn Bhd, Malaysia

Dr. Abdulrahman Ahmad Abdul Muthana - Smart Security Solutions, Yemen

Hatim Mohammad Tahir – Islamic Institute of Higher Education Perlis

Prof. Dr. Rabiah Ahmad - Universiti Teknikal Malaysia Melaka, Malaysia

Dr. Sofia Najwa Ramli - Universiti Tun Hussein Onn (UTHM**)**, Malaysia

FELLOW MEMBERS

Assoc. Prof. Colonel (R) Dato' Ts. Dr. Husin Jazri, Serba Dinamik Group Berhad

Prof. Nabil Sahli, National Agency for Computer Security

HONORARY MEMBER

The Organization of the Islamic Cooperation (**OIC**)

ACRONYMS

A

APCERT	Asia Pacific Computer Emergency Response Team
AUCSEG	AU – African Union Cybersecurity Expert Group

B

BSSN	National Cyber Crypto Agency

C

CAMP	Cybersecurity Alliance for Mutual Progress
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CNCERT	China Computer Emergency Response Team
CPrN	Computer Professionals Registration Council of Nigeria
CSB	Cyber Security Brunei

D

DSA	Defence Space Administration

F

FIRST	Forum of Incident Response & Security Team
FUT	Federal University of Technology

G

GBBL	Galaxy Backbone Limited
GCSCC	Global Cyber Security Capacity Centre
GFCE	Global Forum on Cyber Expertise
GlobalACE	Global Accredited Cybersecurity Education

H

HD	Humanitarian Dialogue

I

ICTA	Information and Communication Technologies Authority
IEEE	Institute of Electrical and Electronics Engineers
ISPAB	Internet Service Provider Association of Bangladesh
IT	Information Technology
ITU	International Telecommunication Union
ITU-ARCC	ITU Arab Regional Cybersecurity Centre

J

JSC “STS”	JSC ‘State Technical Services’

K

KSA	Kingdom of Saudi Arabia

L

LSN	*Lembaga Sandi Negara* / National Crypto Agency
LEA	Law Enforcement Agency

M

MCPD	Mandatory Continuing Professionals Development
MDR	Managed Detection and Response
MDPI	Multidisciplinary Digital Publishing Institute
MISP	Malware Information Sharing Platform
MoU	Memorandum of Understanding
MoCT	Ministry of Communications and Technology
MSSP	Managed Security Service Provider

N

N-CERT	National CERT
NACS	National Agency for Computer Security
NAICOM	National Insurance Commission

NATO	North Atlantic Treaty Organization
NCA	National Communication Authority (Somalia)
NCS	Nigeria Computer Society
NCSC	National Cyber Security Centre
NITDA	National Information Technology Development Agency

O

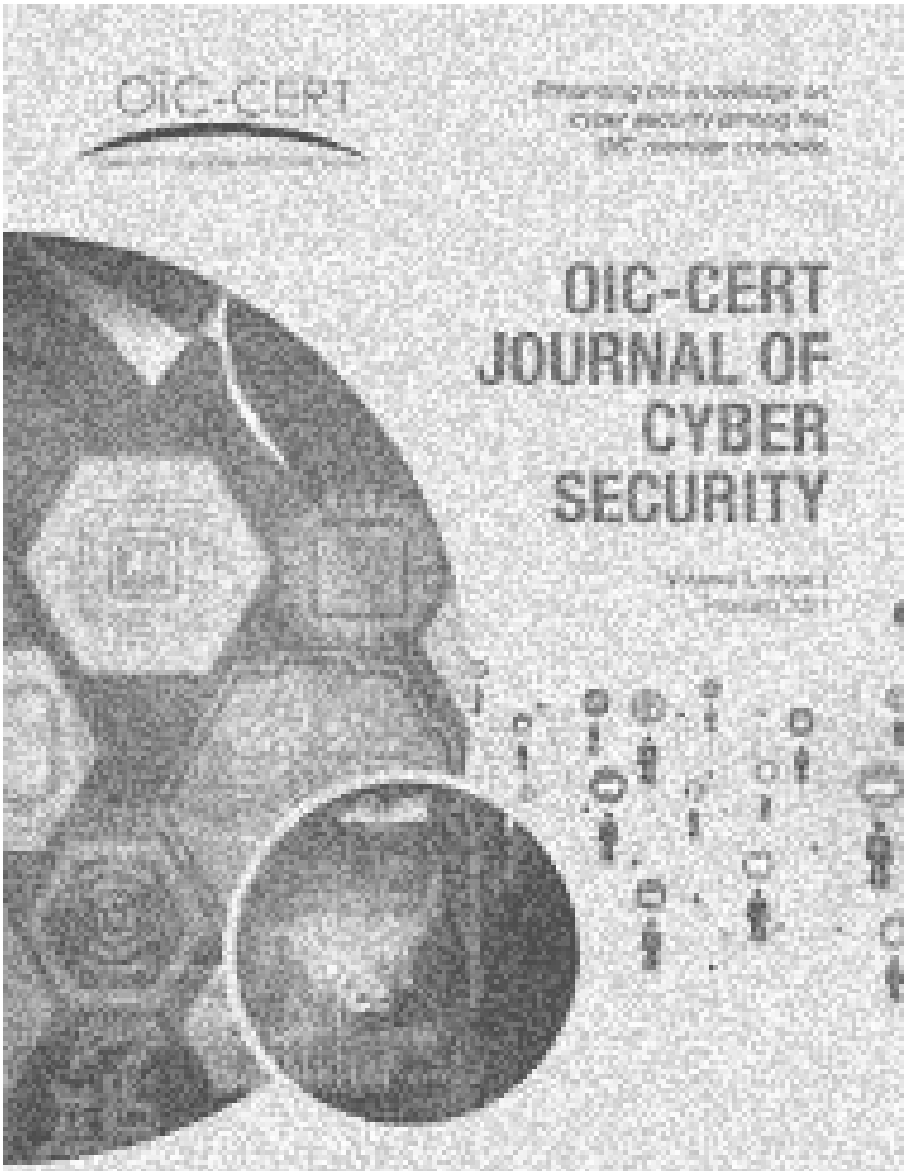
OIC-CERT	Organization of the Islamic Cooperation – Computer Emergency Response Team
OSCE	Organization for Security and Co-operation in Europe

P

PSIRT	Product Security Incident Response Team

S

SaaS	Software as a Service
SOC	Security Operation Centre
SUE	State Unitary Enterprise



OIC-CERT 2020 - In the nutshell

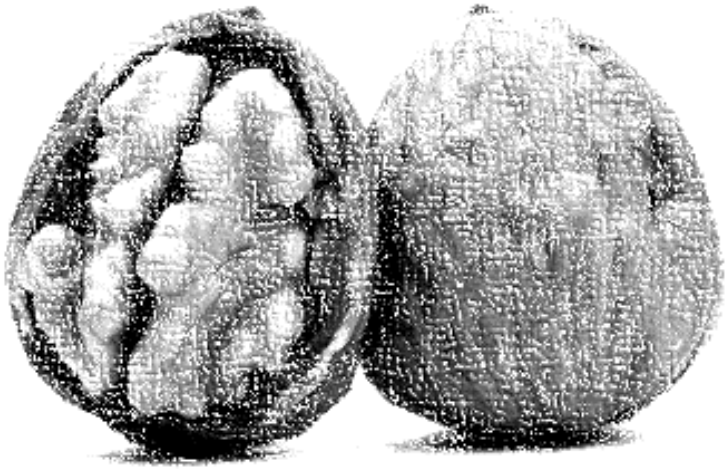
by CyberSecurity Malaysia
The Permanent Secretariat of the OIC-CERT

OIC-CERT Annual Report 2020 consists of members activities done in that year. For this report, 68% of the Full Members participated to share their activities which is the highest so far. Thank you to those who have submitted their reports.

2020 was a challenging year to the OIC-CERT because of the Covid-19 pandemic that pose various challenges for Computer Emergency Response Teams (**CERT**s) around the world. A lot of security incidents happened because cyber criminals use the pandemic issues to create scams and frauds, taking advantage of the public scare towards COVID19 and also due to the increase of online presence because activities that were usually conducted face-to-face were held online instead – the annual conference, general meeting, hands on trainings, and Board face-to-face meetings.

The OIC-CERT now has 53 teams and members from 27 OIC member countries, which is 47% of the OIC member countries. An encouraging number compared to the modest 7 founding members in 2006. In 2020, three new commercial members joined the collaboration - INSIGHT from Oman, TurkCELL from Turkey, and Huawei from UAE. It is a major challenge to get all 57 member states to be on board because of the differing state ICT development level, but OIC-CERT will strive to achieve this goal.

To assist OIC-CERT members in developing their capabilities in facing cyber-threats and the future challenges of the cyber environment, the OIC-CERT Board members were tasked with six (6)



strategic pillars to support OIC-CERT business plan which are:

- Organisation Structure lead by Oman and the Secretariat
- International Cooperation and Promotion lead by Oman
- Standards and Regulations lead by Iran and Egypt
- Technical and Technology lead by Iran and Azerbaijan
- Capacity Building lead by Malaysia and Indonesia
- Awareness lead by UAE

The OIC-CERT 12th Annual Conference 2020 is the pinnacle event of the year. In 2020, the event was held for the first time online since the inception of the OIC-CERT in 2009. More than 200 participants attended the conference worldwide through live broadcast. This is a considerable achievement considering it is the first and having to deal with different logistic and technical challenges. The Secretariat was taken to task in organising this event via online platform.

The OIC-CERT has also conducted the Annual OIC-CERT Cyber Drill 2020 to test and evaluate the readiness and communication capabilities of members in mitigating cyber threats. The drill was conducted together with the 8th Arab Regional Cyber Drill lead by Oman. 25

teams from 24 countries participated including members of FIRST, AfricaCERT and APCERT as OIC-CERT guest participants.

Capacity building is an important facet of cybersecurity in addressing issues related to human capital development at various stages of education. Training is an integral part of capability building. Three online trainings were conducted, one by Malaysia and two by Indonesia which were:

- Managing Technical Journal Online 4th Industrial Revolution – Malaysia
- Managing Security Incident Response during Covid Outbreak: A Lesson Learned – Indonesia
- Responding to Data Breach: Challenges and Strategies - Indonesia

Malaysia has also initiated a unified cybersecurity education program by developing the OIC-CERT Journal of Cyber Security. To date three volumes have already been published. This is an industrial journal, and the Secretariat is always looking for manuscripts especially from information security professionals for future editions. This journal is in the process of being indexed to increase its reputation.

Malware is becoming increasingly sophisticated, intelligent, versatile, available, and is affecting a broader range of targets and devices. Therefore, under the capacity development pillar, Malaysia has developed a Malware research program. From the research program, in 2020, two half year reports on malware research findings were published and six-monthly reports starting from June. Two new participants also joined the program in 2020.

Instilling awareness through cultivating best practices towards creating a resilient environment is another important aspect of cybersecurity. The UAE has conducted six sessions of cybersecurity awareness covering social engineering, malware, mobile security, computer security, social media security, and email security.

Under the Standard and Regulations initiative, a guideline and a list of cybersecurity tools were developed. They were the Security and Privacy Guidelines on Social Network by Iran and Malwares Analysis Tools by Egypt. Under the technical and technology initiatives, Azerbaijan has developed a blacklisting application and awareness measurement for members. Iran has developed an antivirus product available to members who are interested.

This OIC-CERT Annual Report 2020 is a compilation of reports from members that provide the background, highlights of the major activities of the year, achievements, and planned activities of the coming year. This will provide an avenue for members to share their initiatives, success, and their capabilities with others.

MEMBERS' 2020 REPORT

AZERBAIJAN

Azerbaijan Government CERT

Azerbaijan Government CERT (CERT.GOV.AZ)

Background

Azerbaijan Government CERT (**CERT.GOV.AZ**) aids in computer and network security incident handling. It provides incident coordination functions for all incidents involving systems and networks located in the state sector of Azerbaijan Republic.

RFC-2350 - *http://cert.gov.az/en/pages4/rfc-2350.html*

Promo - *https://www.youtube.com/watch?v=tYqPc-lzd54*

Host Organization

Special State Protection Service of Azerbaijan

Special Communication & Information Security State Agency

Establishment

20 Apr 2008

Resources

The Government of Azerbaijan Republic

Constituency

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

2020 Highlights

Summary of Major Activities

Incident Response

CERT.GOV.AZ will assist system administrators in handling the technical and

organizational aspects of the incidents. Aiding or advising with respect to the following aspects of incident management.

Incident Triage

- Investigating whether indeed an incident has occurred
- Determining the extent of the incident

Incident Coordination

- Determining the initial cause of the incident (the vulnerabilities exploited)
- Facilitating communication with other sites which may have be involved
- Making reports to other Computer Emergency Response Teams (**CERT**s) / Computer Security & Incident Response Teams (**CSIRT**s) teams
- Composing announcements to users, when applicable

Incident Resolution

- Removing the vulnerabilities
- Liquidation of consequences of the incident
- Evaluating possible additional actions, considering the cost and risk
- Provide assistance in evidence collection and data interpretation when needed

In addition, CERT.GOV.AZ will collect statistics concerning incidents and will notify the community to assist in protecting against known attacks.

Proactive Activities

Information services

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

Training services

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

"Faced over 3000 cyber-attacks during the 44 days of the Patriotic War"

CERT.GOV.AZ Contact

Representative mail. *rep@cert.gov.az*
Group mail. *team@cert.gov.az*
General use. *info@cert.gov.az*
Tel. +994 12 435 28 25
Fax. +994 12 435 28 31

2020 Activities, Achievements, & Events

Recorded and handled 4989 incidents

Provided 244 Audit / Penetration Test (**Pentest**) for required government bodies

Updated the user list on the OIC-CERT Awareness System and provided 2 system tests

Updated the required workflow in the OIC-CERT Membership Portal

Conduct training for all Point-of-Contacts (**PoC**s) of government bodies on cybersecurity subjects

Published İnformation Security Journal for free for government bodies

Faced over 3000 cyber-attacks during the 44 days of the Patriotic War

Hold 1st Global Defence Technology Hackathon in Azerbaijan after 44 days of the Patriotic War - *https://globaldeftech.com/en*

Posted alerts about 40 Advance Persistance Threats (**APT**s) attacks, and also participated in several TV programs to raise awareness

Worked on a new algorithm to measure government bodies' security and awareness indexes

Participated in different online local and international conferences, meetings, and courses i.e.Organization of the Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**), Forum of Incident Response & Security Team (**FIRST**), and Organization for Security and Co-operation in Europe (**OSCE**)

2021 Planned Activities

Integrate the OIC-CERT membership and awareness test portals

Integrate SIM3 Self-Assessment Tool for Security Incident Management Maturity Model into the OIC-CERT membership portal

Work on the functionality to make the *blacklist.gov.az* service more practical to use and publish new versions of the *blacklist.gov.az* service

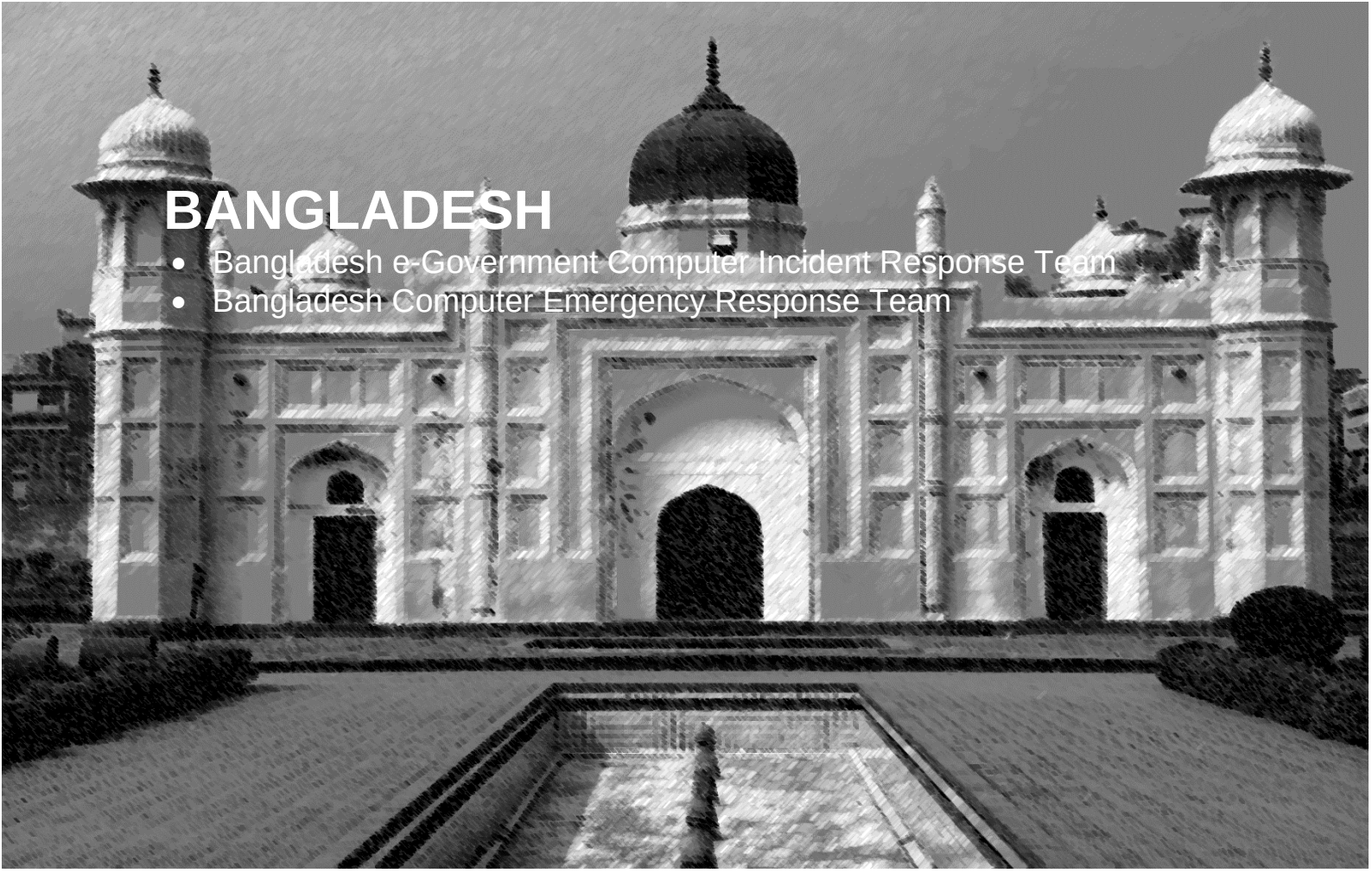
Holding the 2nd Global Defence Technology Hackathon

Continue collaboration with CERTs internationally

https://www.youtube.com/watch?v=Agf9zRsf008

https://xritda.gov.az/az/journal

https://www.youtube.com/watch?v=lD4MI-gJbMg



BANGLADESH

- Bangladesh e-Government Computer Incident Response Team
- Bangladesh Computer Emergency Response Team

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

Background

Bangladesh e-Government Computer Incident Response Team (**BGD e-GOV CIRT**) is acting as the National CERT of Bangladesh (**N-CERT**) currently with responsibilities including receiving, reviewing, and responding to computer security incidents and activities. Under the Government of the People's Republic of Bangladesh, BGD e-GOV CIRT reviews and takes the necessary measures to resolve the issue with broad cybersecurity ramifications, conducts research & development, and provides guidance on security vulnerabilities.

BGD e-GOV CIRT also work with various government units, Critical Information Infrastructures (**CII**), financial organizations, law enforcement agencies, academia, and civil society to help improve the cybersecurity defence of Bangladesh.

Establishment

The process to establish BGD e-GOV CIRT started in November 2014 and the team starts the operation in February 2016.

"Bangladesh rank has improved 8 places to 65th on the National Cyber Security Index"

Resources

Currently 16 people are working in BGD e-GOV CIRT and more will be joining.

Constituency

The Constituency 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 N-CERT of Bangladesh with a mandate to serve the whole of Bangladesh.

2020 Highlights

Summary of Major Activities

BGD e-GOV CIRT has successfully organized the country's First National Cyber Drill 2020

BGD e-GOV CIRT has successfully organized Cyber Drill 2020 for the financial institution to strengthen their incident handling process

Bangladesh has improved by eight places to rank 65th among the 160 countries on the National Cyber Security Index

COVID-19 Minimizing IT Data Centre Risk Plan Report was prepared

Blockchain Technology Based Certificate Management and Verification System was developed

1119 cyber security incident registered in the tracking system

Total 1145 government, non-government, and other officials have been trained on cybersecurity

National Cyber Drill 2020 organizer team BGD e-GOV CIRT

2020 Achievements

BGD e-GOV CIRT took part in the annual Capture The Flag (**CTF**) event organized by FIRST.Org and achieved 19th position among 278 teams from all over the world

BGD e-GOV CIRT has successfully participated in the OIC-CERT Cybersecurity Drill 2020 and achieved 85% score

Activities & Operations

Events organized by the organization / agency

Online workshop on Cyber Threat Landscape of Bangladesh

Training session on cyber-crime, social media awareness, and security measures held in the Department of Women Affairs

Hands-on training session on Domain Name System (**DNS**) and Domain Name System Security Extension (**DNSSEC**) Deployment

Special training on Cybersecurity, arranged by Startup Bangladesh

Event involvement

Participated in The Global Cybersecurity Forum Conference-2020 - *Riyadh, Saudi Arabia*

Attended the program on Cybersecurity Studies arranged by George C. Marshall European Centre for Security Studies - *online*

Global Cybersecurity Centre for Development (**GCCD**) Cybersecurity Seminar organized by KISA - *online*

Cybersecurity Capacity Building Conference 2020 - *Australia*

Participated in *Empower the Modern IT with Integrated Security Portfolio* - *Thailand*

Participated in *Modernizing your cyber security architecture: towards professional CSIRT/SOC* - *online*

Participated in *Cellebrite Analytics Desktop and Cellebrite Byte-size Learning* - *online*

Participated in the 2020 Asia Pacific Information Security Conference (**APISC**) Security Training course by Kr-CERT/CC

Achievements

Provided 98 cyber sensor analysis reports (from Jan 2020 - Dec 2020) to multiple CII

'*Cyber Threat Intelligence Report*' provided to 55 government and non-government organizations

'*Malware Threat Intelligence Report for Bangladesh Context*' was prepared and published

BGD e-GOV CIRT published *Cyber Threat Landscape Report 2020*

Total 283 reports on social media monitoring

282 cyber security advisories and news published on the BGD e-GOV CIRT website as awareness to the people about cybersecurity

Publishing monthly cybersecurity magazines for the stakeholders

2021 Planned Activities

Arrange cyber drills for different sectors

Perform risk assessment to CIIs

Provide training on industrial control system (**ICS**) for the Public sector

Perform vulnerability assessment and penetration testing for the financial sector

Training and workshop on cybersecurity for government organizations

Provide regular cyber sensor analysis reports (intrusion & suspicious activities) to CII where the cyber sensors are deployed

BGD e-GOV CIRT SOC visited by Hon'bl ICT State Minister

BGD e-GOV CIRT Team meeting with Hon'bl ICT State Minister

National Cyber Drill 2020 prize awarding ceremony inaugurated by Hon'bl ICT State Minister

National Cyber Drill 2020 visited by Bangladesh Air Force Officials

Training session on cyber-crime, social media awareness & security measures

Participated in the 2020 APISC Security Training Course by KrCERT/CC

BGD e-GOV CIRT Team

Bangladesh Computer Emergency Response Team (bdCERT)

Background

Bangladesh Computer Emergency Response Team (**bdCERT**) is the Computer Emergency Response Team for Bangladesh and is the primary PoC for handling incidents in Bangladesh. The teamwork towards improving the Internet security in the country. One of the tasks is to provide information about threats and vulnerabilities that could affect the users.

bdCERT work closely with various organizations and associations such as:

- The Internet Service Provider Association of Bangladesh (**ISPAB**)
- The Bangladesh Association of Software & Information Services (**BASIS**)
- The Bangladesh Civil Service (**BCS**)
- The South Asia Network Operators Group (**SANOG**)
- The Bangladesh Telecommunication Regulatory Commission (**BTRC**)
- The law enforcement agencies

to mitigate cyber-attacks that are either originating from Bangladesh or external. The team provide training and awareness programmes in information security and issues affecting Internet security in Bangladesh.

Establishment

bdCERT was formed in July 2007. It is a non-government and not for profit organization and the members work on voluntary basis. It was founded by a few motivated network professionals working in the Internet service provider companies for many years.

The team had been affected by virus attacks and cyber-crimes but did not know how to deal with it thus the need for a CSIRT arises. Therefore, these professionals came together and formed bdCERT to handle cyber incidents in the country.

Resources

Since bdCERT is a voluntary organization, it often faces resource scarcity. Currently the team consists of 6 working team members providing security alerts to users via the website and mailing lists.

Constituency

The constituency of bdCERT is all the Internet user communities of Bangladesh. The team work closely with all the ICT stakeholders, particularly with ISPAB and with relevant government bodies and law enforcement agencies to mitigate Internet threats.

2020 Highlights

Summary of Major Activities

In 2020, bdCERT conducted security incident handling and published alerts on the latest cyber threats, vulnerabilities, and best practices.

Activities & Operations

Events organized by the organization / agency

Due to Covid-19 pandemic and resource constraints, bdCERT was unable to organize any events.

Events involvement

Participated in numerous distance training conducted by the OIC-CERT and the Asia Pacific Computer Emergency Response Team (**APCERT**)

The online training titled '*Remote Working Security*' by aeCERT was most useful in view of Covid-19 pandemic – *29 Apr 2020*

Participated in the online conference on '*CNCERT International Partnership in Emergency Response*' by CNCERT – *16 Dec 2020*

2021 Planned Activities

Increase organizational capacity

Enhancing CSIRT services

"The teamwork towards improving Internet security in the country"

BRUNEI DARUSSALAM

Brunei Computer Emergency Response Team

Brunei Computer Emergency Response Team (BruCERT)

Background

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

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

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

The Brunei Computer Emergency Response Team (**BruCERT**) was established in May 2004. It was formed in collaboration with the Authority for Infocommunications Technology Industry (**AITI**), 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 CSB.

Services

24 x 7 security related incidents and emergency response from BruCERT

24 x 7 security related incidents and emergency response on-site (deployment of response is within 2 hrs after an incident report is received). This service only applies to BruCERT constituents

Broadcast alerts (early warning) of new vulnerabilities, advisories, viruses, and security guidelines from BruCERT's website. BruCERT constituents will receive alerts through email and telephone as well as defence strategies in tackling IT Security related issues

Promote security awareness programmes to educate and increase public awareness and understanding on information security and technical know-how through education, workshops, seminars, and trainings

Establishment

BruCERT coordinates with the local and international CSIRTs, network service providers, security vendors, law enforcement agencies, as well as other related organizations to facilitate the detection, analysis, and prevention of security incidents on the Internet.

Workforce

BruCERT currently has a strength of 66 staff (100% local) of which a majority specializes in information technology (**IT**) and the rest is administration and technical support. The staffs have undergone training on various IT and security modules, such as:

- A+,
- N+
- Linux+
- Server+
- Security+, Security Certified Network Professional (**SCNP**)
- Security Certified Network Administrator (**SCNA**)
- Certified Internet Web Professional (**CIW**)
- Certified Ethical Hacker (**CEH**)
- Cisco Certified Network Associate (**CCNA**)
- Certified Information Systems Security Professionals (**CISSP**)
- BS7799 Implementer

SANS trainings such as:

- GIAC Reverse Engineering Malware (**GREM**)
- GIAC Certified Intrusion Analyst (**GCIA**)
- GIAC Certified Incident Handler (**GCIH**)
- GIAC Certified Forensic Analyst (**GCFA**)
- GIAC Penetration Tester Certification (**GPEN**)

Most of BruCERT workforce are certified in at least one of these certifications.

Constituency

BruCERT has close relationships with government agencies, a major ISP, and various numbers of vendors.

The Government Ministries and Departments

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

The 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 the IT Central Procurement, Network Central Procurement, Co-location, ONEPASS (a PKI initiative), and Co-hosting are provided by EGNC. BruCERT work closely with EGNC in

providing incident response and security monitoring since most of the government equipment resided at EGNC.

The Authority for Info-communications Technology Industry of Brunei Darussalam

Authority for Info-communications Technology Industry of Brunei Darussalam **(AITI**) is an independent statutory body to regulate, license, and develop the local ICT industry. This agency also manages 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.

Royal Brunei Police Force and other Law-Enforcement Agencies (LEAs)

BruCERT has been collaborating with the Royal Brunei Police Force (**RBPF**) and other law enforcement agencies (**LEA**s) to resolve computer related incidents through the Digital and Mobile Forensic services.

Unified National Network

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

Contact

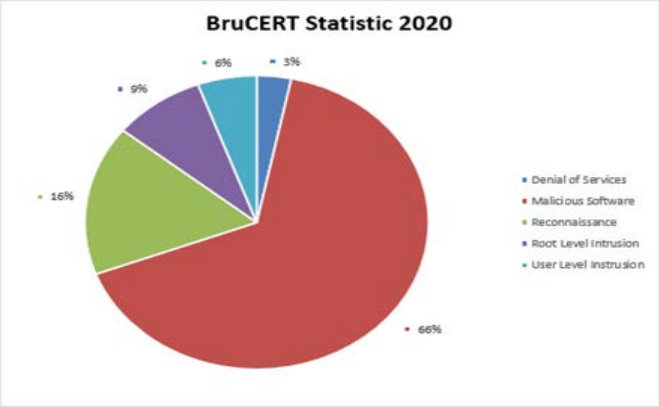
BruCERT Coordination Centre welcome reports on computer security related incident, which can be reported to:

Tel: +(673) 245 8001
Fax: +(673) 245 8002
Email: *cert@brucert.org.bn*

2020 BruCERT Operation

Incident response

In 2020, BruCERT received a lot of reports from the public as well as from BruCERT security intelligent sensors. Malware infections are the most common cyber threats in Brunei Darussalam, where there are few cases involving Ransomware especially the "*Ryuk*" type of ransomware. There are an increase in Denial of Service (**DoS**) attacks as well as reconnaissance compared to the previous year. The statistic of the security incident is shown in the following diagram.

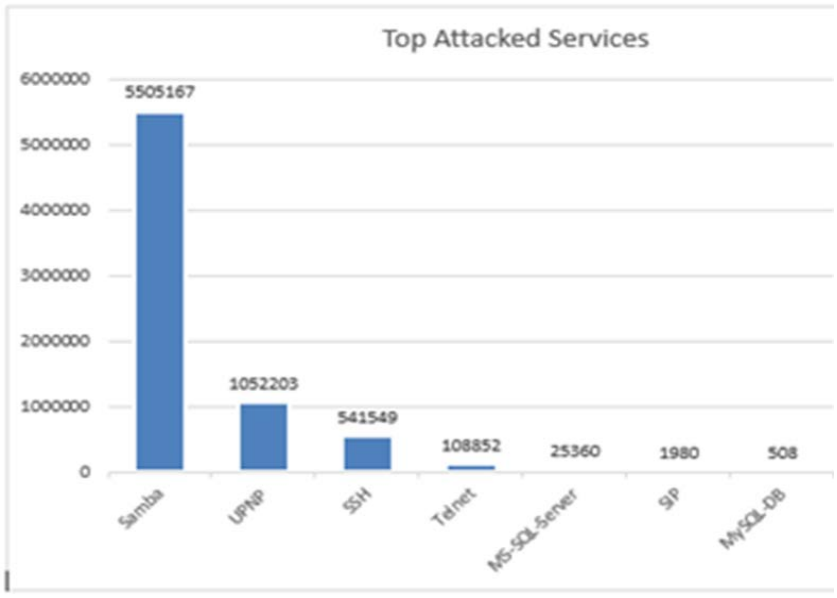


TYPE OF ATTACK	COUNT
Denial of Services	174
Malicious Software	3553
Reconnaissance	889
Root Level Intrusion	465
User Level Intrusion	299

BruCERT Honey Pot

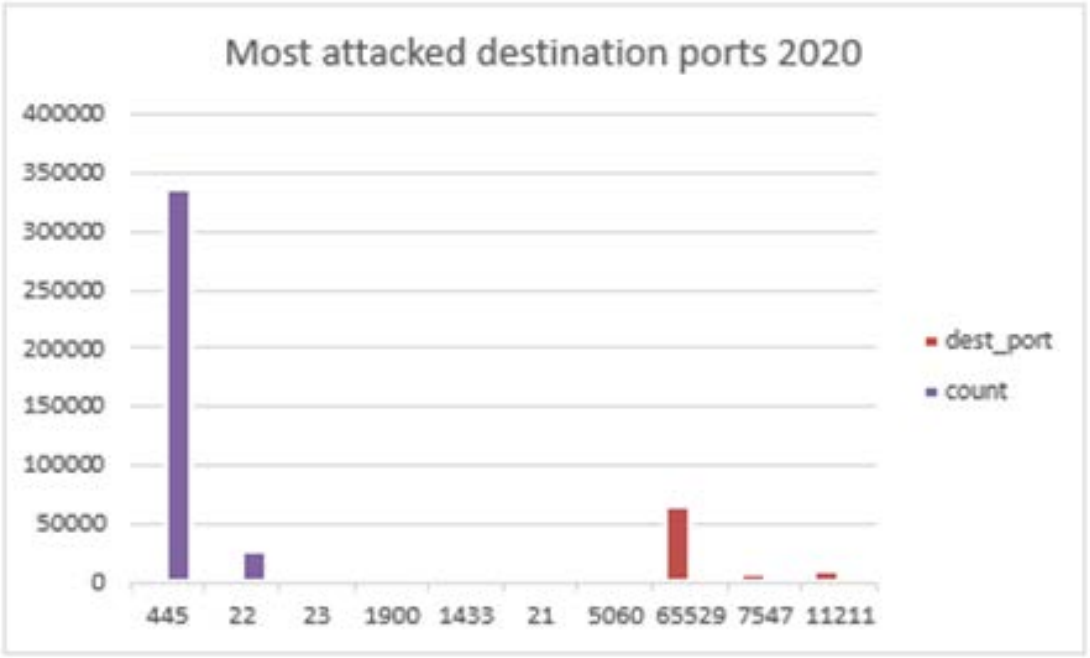
In the year 2020, the most attack services which were recorded by BruCERT Honey Pot sensor was Samba services numbering around 5,505,167 attacks. The total of attacks on services which was recorded is 7,235,619.

The following graph and table show the breakdown of the figures.



EVENT	COUNT
Samba	5,505,1674
UPNP	1,052,203
SSH	541,549
Telnet	108,852
MS-SQL-Server	25,360
SIP	1,980
MySQL-DB	508

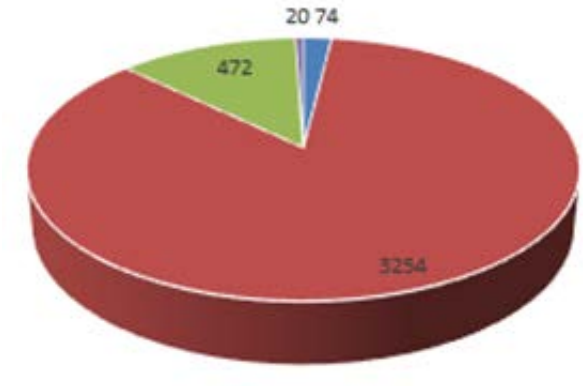
The most abused port number is 445, which in this case used by SAMBA (**SMB**). The second abused port is port number 1433 which used by Microsoft SQL server for database management. It is assumed the attack on SMB might came from "*WannaCry Ransomware*", trying to exploit the vulnerability.



Port No	455	22	23	1900	1433	21	5060	65529	7547	11211
Count	337,252	26,140	4,777	4,652	1,707	939	80	58	28	24

BruCERT honeypot managed to capture some of the malware hashes, the following figure and table shows the summary of the most detected malware in BruCERT Honeypot.

Top Malware Detected 2020



MALWARE TYPE	COUNT
Generic Trojan	74
Coinminer	3254
Ransomware	472
Unknown	20
TOTAL	**3820**

"There are an increase in Denial of Service (DoS) attacks as well as reconnaissance compared to the previous year"

2020 Highlights

Seminars / Conferences / Meetings / Visits

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

EGYPT

Egypt Computer Emergency Readiness Team

Egypt Computer Emergency Readiness Team **(EG-CERT)**

Background

Egypt Computer Emergency Readiness Team (**EG-CERT)** was established in Apr 2009 as part of the National Telecom Regulatory Authority (**NTRA**).

Establishment

EG-CERT is tasked with providing computer and information security incident response, support, defence, and analysis against cyber-attacks. The agency has established collaboration relationship with the government, financial entities, and any other CII sectors of Egypt with the mission to provide early warning systems against malware spreading and massive attacks targeting the Egyptian CII.

Resources

Incident handling
Malware analysis
Penetration testing
Digital forensics
Cyber security awareness
Wireless security

Constituency

The Egyptian National Telecom Regulatory Authority.

2020 Highlights

Summary of Major Activities

Regular incident handling within the constituency

Malware analysis of various types of malware samples

Issuing threat intelligence reports

Performing penetration testing on CII

Several other activities that are related to increasing the level of security in Egypt

Since the issuance of the e-crime law in August 2018, the digital forensics department has been receiving an increasing number of cases for forensic analysis, the department received and conducted analysis for more than 30 cases in 2020

The Security Operation Centre (**SOC**) team is making tangible progress in the centre building process

The Awareness team has been active on social media this year and have postings on technical and general awareness content

2020 Achievements

Managed to handle many incidents and mitigated the risk of several critical incidents

Managed to issue malware reports and intelligence reports and to create removal tools for several malwares affecting the constituency

Managed to patch many vulnerable critical systems under the constituency

Activities & Operations

Events organized by the organization / agency

Organized the Sectoral Incident Response Centre Cadre Development Program, which is a high-level training event for the sectoral CERT teams.

Events involvement

The event was fully organized by EG-CERT.

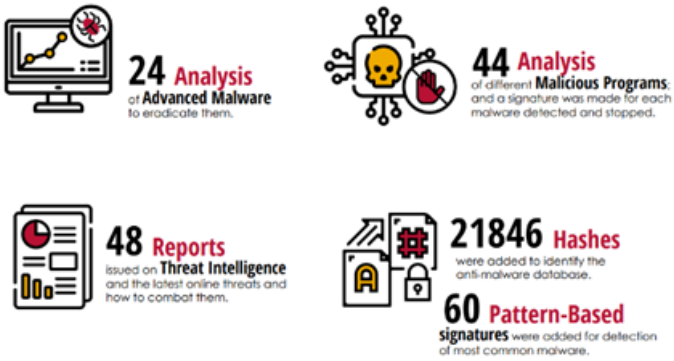
Achievement

The event was a success.

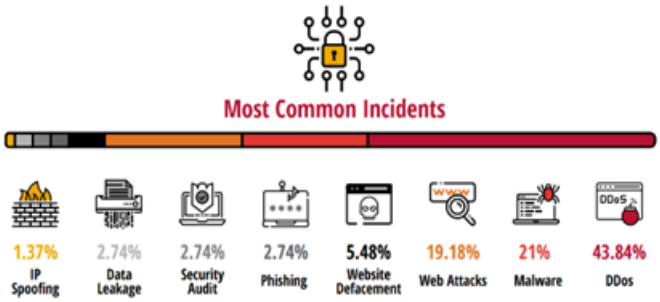
2021 Planned Activities

Full deployment of the SOC.

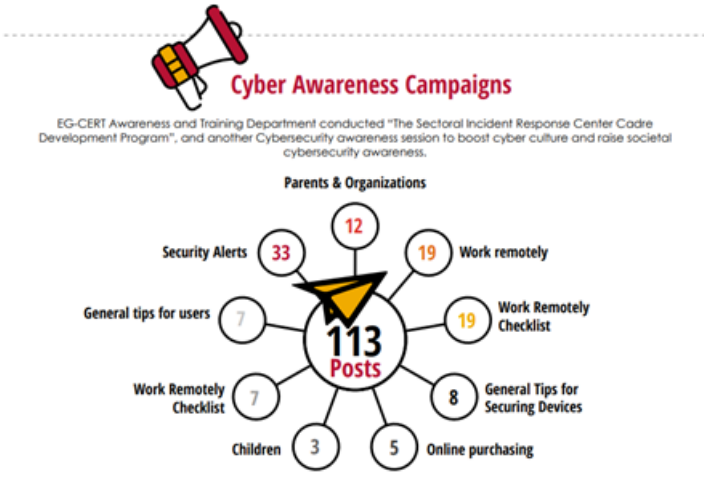
Please note that some of the following statistics are exclusive to Q3 & Q4 2020



Malware analysis



Awareness



INDONESIA

National Cyber and Crypto Agency

National Cyber and Crypto Agency **(BSSN)**

Background

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 no 26 in 2007. Since the establishment until 2018, Id-SIRTII/CC assumed the function as the National CSIRT and Coordination Center for national incident handling and works under the Directorate of Telecommunication of the Ministry. Based on the Presidential Decree no 53 in 2017, Id-SIRTII/CC merged and moved to the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara* - **BSSN**).

In April 2018, BSSN 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**).

Establishment

ID-SIRTII/CC was established on 4 May 2007 and later merged with LSN to make a new national agency named BSSN. This is based on the Presidential Decree no 53 in 2017 and BSSN officially started in April 2018.

Resources

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

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.

2020 Highlights

Summary of Major Activities

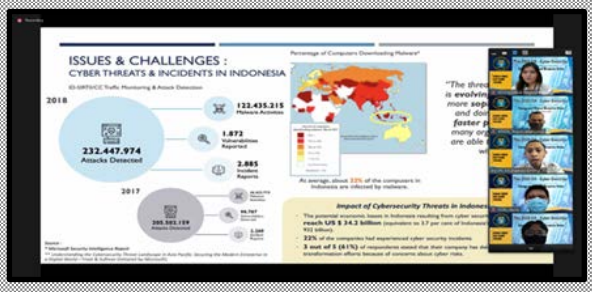
The COVID-19 pandemic has been the headline over the past years. This pandemic has also forced organizations and individuals to embrace new practices such as social distancing, hand washing & sanitizing, and remote working. Governments are reconsidering ways to ensure that their countries are stable by developing and enforcing new economic plans and focused on the health during this crisis.

In 2020, Indonesia had conducted several activities related to cybersecurity such as improving the national cyber capacity as well as strengthening the collaboration and coordination. Active involvement and contribution in the region are maintained such as in ASEAN, Asia Pacific, OIC and any global forum.

In terms of the OIC-CERT, Indonesia has a main role with Malaysia to contribute to the capacity building program as part of the OIC-CERT strategic pillars. The United Arab Emirates (**UAE**) also support this strategic pillar by conducting several online trainings for members of the OIC-CERT. Generally, all programs can effectively run during this pandemic.

Based on our national cybersecurity monitoring and incident report, there were no large-scale network security incident happened with mass damage, but it is very important to increase the attention level to maintain security while employees are working from home during this pandemic. Thus, it is necessary for the government, ISPs, the society, and Internet users to pay more attention and cooperation with each other. There is also the need of increasing the number of collaborations with CERTs in the region as well as in the global community to prevent and mitigate the impact of any cyber threat.

ASEAN - Japan Cyber Exercise 2020



CII Cyber Exercise 2020

ACID 2020

Workshop Managing CSIRT for Government

2020 Achievements

The major achievement in 2020 are the establishment of 15 CSIRT organization for the government sector, and a CSIRT organization for the CII sector.

Activities & Operations

Events organized by the organization / agency

Cybersecurity Drill (Cyber drill for the government agencies and CII sectors)

Cybersecurity Exercise for the CII sector

Amazing Trace for the CII Sector

Hands-on Workshop and Training (Data Breach, Malware Handling, Digital Forensic; and Managing CSIRT)

Conferences, Seminars, and Forum Group Discussion of the Government Sectors

Events involvement

Participated in the ASEAN - JAPAN CYBER EXERCISE 2020 - *25 Jun 2020*

Conducted the Workshop for Managing CSIRT for the Government Sector - *8 Jul 2020*

Conducted the Critical Information Infrastructure Cyber Exercise - *11 & 12 Aug 2020*

Conducted the OIC-CERT online training '*Managing Security Incident Response During Covid Outbreak: A Lesson Learned*' - *3 Sep 2020*

Participated in the Arab Regional and OIC-CERT Cyber Drill - *22 Sep 2020*

Participated in the ASEAN CERT Incident Drill (**ACID**) 2020 - *7 Oct 2020*

Conducted the OIC-CERT online training: '*Responding to Data Breach: Challenges and Strategies*' - *27 Oct 2020*

Participated in ITU Cyber Exercise - *27 Oct to 5 Nov 2020*

Achievements

The major achievements in 2020 are the establishment of 15 CSIRT organization for the government sector, and a CSIRT organization for CII sector as well as improving the capacity of human resources in cybersecurity skills and competences.

There are various activities on cyber drill for specific sectors conducted to increase the level of coordination and readiness in facing cybersecurity incidents.

2021 Planned Activities

Due to the implementation of the Electronic-based Government System as a nationwide policy, Indonesia is accelerating the establishment of CERTs / CSIRTs for local government (provinces) as well as encouraging the CII related sectors.

OIC-CERT Online training

KAZAKHTAN

Kazakhtan Computer Emergency Response Team

Kazakhstan Computer Emergency Response Team (KZ-CERT)

Background

Kazakhtan Computer Emergency Response Team (**KZ-CERT**) is the single centre for national information systems users and Internet segment providing collection and analysis of security incident reports as well as consultative and technical assistance to users in preventing cyber threats.

KZ-CERT has signed Memorandum of Understanding (**MoU**) with the following CERTs and international organizations:

- CERT-In, India
- RU-CERT, Russian Federation
- UZ-CERT, Uzbekistan
- CERT.AM, Armenia
- CyberSecurity Malaysia, Malaysia
- CERT.LV, Latvia
- CERT-Lt, Lietuve
- CERT.GOV.AZ, Azerbaijan
- CERT Australia, Australia
- Operations and Analysis Centre under the President of the Republic of Belarus, Belarus
- Team Cymru Community Services, USA
- CNCERT/CC, China
- KISA, Korea
- Kaspersky Lab, Russian Federation
- Positive Technologies, Russian Federation
- Check Point Software Technologies Ltd., Israel

The JSC 'State Technical Services' (**JSC 'STS'**) has signed MoUs with the following:

- LEPL Data Exchange Agency of the Ministry of Justice of Georgia, Georgia
- The Israeli National Cyber Directorate of the state of Israel, Israel
- ID-CERT, Indonesia
- THALES Six GTS France SAS, France

Establishment

KZ-CERT was established in 2011 and today operates under JSC 'STS'.

Resources

As of March 2021, KZ-CERT has over 23 employees.

Constituency

The constituency of KZ-CERT is Kazakhstan's cyber community.

2020 Highlights

The number of cybersecurity incidents in 2020.

	TYPE OF INCIDENT	INCIDENT COUNT
1	Botnets	11780
2	Lack of access to the Internet resources	2888
3	Phishing – Internet / Telephone / phishing / Scamming	1419
4	Creation and distribution of malware	661
5	Others	1032
6	Unauthorized access / content modification	291
7	DoS	297

Summary of Major Activities

JSC "STS" carries out the following types of activities, classified as state monopoly, in the field of informatization. This is done in accordance with Article 7-4 of the Law of the Republic of Kazakhstan dated 24 Nov 2015, No. 418-V 'On Informatization':-

Assisting owners and users of informatization facilities in the safe use of information and communication technologies

Providing interaction between the operation and industry centres for information security of the financial market and financial organizations

Collecting, analysing, and summarizing information from operation centres on information security incidents mainly regarding the communication infrastructure of the 'electronic government'

Carrying out intersectoral coordination regarding the monitoring of information security, protection, and safe functioning of informatization facilities of the 'electronic government', the Kazakhstan segment of the Internet, and critical objects of information and communication infrastructure. This is done when responding to information security incidents with joint information security measures following the guidelines determined by the legislation of the Republic of Kazakhstan

Taking measures to identify, suppress, and investigate threats and incidents of information security involving the informatization of the 'electronic government' and formulates recommendations for mitigation and prevention

2020 Achievements

According to the ITU Global Cybersecurity Index 2018/2019 Report, the Republic of Kazakhstan is ranked 40th in cybersecurity implementation.

The position in the cybersecurity index was influenced by the joint efforts of the government bodies, non-governmental organizations etc. In particular, the basic conceptual approaches to the country's cybersecurity sphere are to develop and approve:

A number of legislative acts

The Cybershield of Kazakhstan cybersecurity concept

Testing laboratories in the field of information security

Malicious code research

The National Information Security Coordination Center

Activities & Operations

Events involvement

32nd Annual FIRST Conference - *online*

OIC-CERT 12th Annual Conference 2020 - *online*

NatCSIRT 2020 Carnegie Mellon University - *online*

eCrime 2020 – Symposium on Electronic Crime Research - *online*

The 2nd International Symposium on Industrial Cybersecurity Emergency Response - *online*

Achievements

KZ-CERT joined APCERT as a liaison partner.

2021 Planned Activities

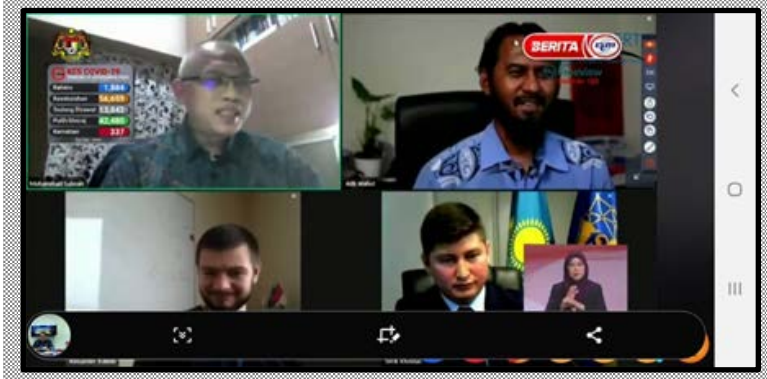
To strengthen the collaboration with other CERTs and international companies in the field of information security incidents response

To build the cooperation and to sign MoU on information security incidents response in order to create the necessary legal and organizational conditions for mutually productive beneficial cooperation in this field with other CERTs and international companies

To develop and utilize the Malware Information Sharing Platform (**MISP**) for sharing, storing, and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information, or even counter-terrorism information

To participate in training, conferences, meetings etc. within the framework of international collaboration to exchange experience on information security incidents handling, methodology, and preparedness

ITU GLOBAL CYBERSECURITY INDEX 2018/2019 REPORT, THE REPUBLIC OF KAZAKHSTAN IS RANKED 40TH IN CYBERSECURITY



OIC-CERT 12th Annual Conference 2020

KUWAIT

Kuwait National Cyber Security Centre

Kuwait National Cyber Security Centre (NCSC)

Background

National Cyber Security Centre (**NCSC**) of the state of Kuwait is the body for all cybersecurity initiatives of the country. After the publishment of the National Cyber Security Strategy for the state of Kuwait 2017-2020, the centre is tasked to develop the framework, operating model, and programme for the State of Kuwait focusing on the main objectives as follows:

- Promote a culture of cyber security that supports safe usage of the cyber space
- Safeguard and continuously maintain the security of national assets
- Promote the cooperation and information exchange among local and international bodies in cybersecurity

Establishment

Translating the initiatives stated in the National Cybersecurity Strategy of the state of Kuwait into operational tasks to secure Kuwait

Organizing with different CIIs and international organizations in setting the base ground for enhancing the Kuwait National Cybersecurity Centre

Resources

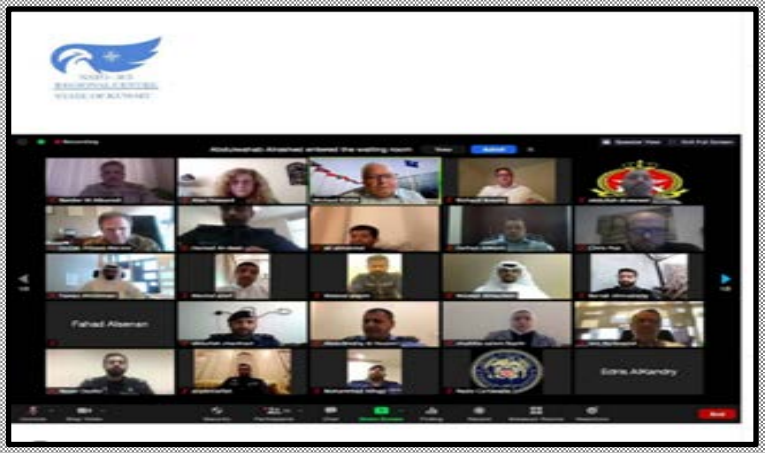
Currently the unit consists of a few people, however recruitment will be done as soon as the COVID-19 issues are resolved.

Constituency

CITRA is the national CERT for the State of Kuwait.

CERC Invitation

Kuwait Threat Hunter 2020 announcement & winner



NATO ICI Center online training

2020 Highlights

Summary of Major Activities

Establish and promote a national cyber security structure, including capacity development and awareness with all CII to secure Kuwait.

2020 Achievements

Cyber security awareness programme for CITRA

Cyber security awareness for the public

Organize for universities to offer post graduate degrees in cybersecurity

Organize the 2nd research and education CERC2020 event in the field of cybersecurity

Conduct several workshops and training for technical employees in the field of cybersecurity

Establish COVID-19 initiatives

Activities & Operations

Events organized by the organization / agency

Cybersecurity Education & Research Conference CERC2020

Threat Hunters 2020 Competition in partnership with ITU Arab Regional Cybersecurity Centre (**ARCC**)

Several online webinars

Events involvement

Participation in the Oman Tech event

Participation in the Kuwait Tech event

Participation in several training arranged by NATO school

Participation with other entities in preparing several policies during the COVID-19 pandemic on data privacy for healthcare applications

Participation in the USARCENT BCW2020 Virtual Competition

Achievements

NCSC service to block inappropriate web content or applications online

Information sharing platform within CIIs

Establishing the initiative to review the security of new established government applications during COVID-19 pandemic

Establishment of remote working policy

2021 Planned Activities

The NCSC is currently in the final phase in starting the national cybersecurity program within Kuwait. The NCERT will be the main backbone for this programme with additional functions that will be included within this programme. The NCERT will also join the global CERT networks and continue to build and maintain relationships with national and international CERTs.

A continuation to study and assess the national cyber security maturity levels and further developing CERT employees' levels of cybersecurity expertise in order to manage and handle the National CERT Programme.

Social Media Awareness post

KYRGYZSTAN

Kyrgyz Republic Computer Incident Response Team

The Coordination Center for Cybersecurity of the State Committee for National Security of the Kyrgyz Republic (CERT-KG)

Background

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

Establishment

CERT-KG was established on 21 May 2020.

Resources

Government.

Constituency

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

2020 Highlights

Summary of Major Activities

Making proposals for the development of a cybersecurity policy

Coordination of activities for organizations, centres for responding:

- to computer incidents (departmental, industry, and others)
- to ensure security and identify cybersecurity
- identify, prevent, and suppress computer attacks
- respond to computer incidents

Identification, prevention, and suppression of possible cybersecurity threats

Making suggestions to improve the legislation of the Kyrgyz Republic in the field of cybersecurity operations

Participation in the development of international treaties for the Kyrgyz Republic in the field of cybersecurity

Ensuring the fulfilment of obligations in international relations especially on activities are carried out by the Kyrgyz Republic

Completion of tasks in accordance with regulatory legal acts of the Kyrgyz Republic

2020 Achievements

As part of the implementation of the roadmap for the Digital Transformation Concept '*Digital Kyrgyzstan 2019-2023*', CERT-KG was established within the Coordination Centre in ensuring cybersecurity of the Kyrgyz Republic.

By the Order of the Government of the Kyrgyz Republic No. 380-r dated 23 Nov 2020, the '*Interdepartmental Commission on Information and Cybersecurity*' was established, which is a permanent consultative and advisory body formed to create conditions and coordinate actions of the state bodies and local self-government bodies in the field of information and cybersecurity.

The Coordination Centre for Cybersecurity of the State Committee for National Security of the Kyrgyz Republic conducts a few technical measures to detect computer attacks on the information systems of state bodies of the Kyrgyz Republic.

Activities & Operations

Events organized by the organization / agency

CERT-KG conducted cyber orders for the state bodies of the Kyrgyz Republic - Oct 2019.

Events Involvement

Participation in the regional event '*Cybersecurity*' of the ITU for the Commonwealth of Independent States (**CIS**) member states

Participation in the regional event on the investigation of combating crime in the field of information and communication technologies organized by the OSCE

Participation in the CyberDrill Global Cyber Training organized by the ITU

Participation in the event '*CyberCrimeCon Virtual 2020!*' organized by GROUP-IB

Participation in the virtual seminar '*Studying the cyber experience of the Republic of Korea: A virtual study visit to KISA*'

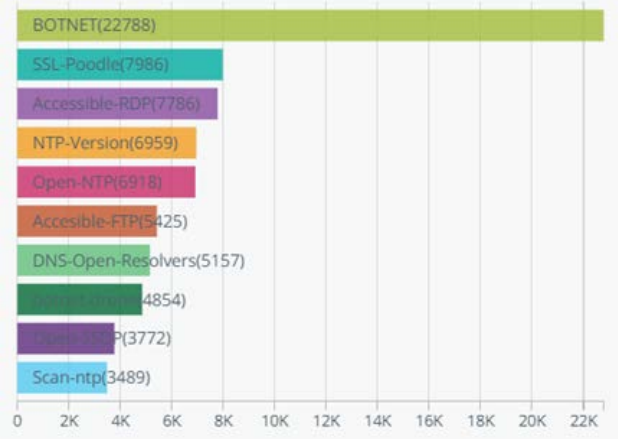
Participation in a meeting on cybersecurity issues organized by the the Turkic Council for Information and Communication Technologies

Participation in the OSCE-Wide Cyber / ICT Security Conference 2020 '*Fostering Co-operation for a Stable Cyber / ICT Environment*'

2021 Planned Activities

Organize and conduct the first national cyber-studies '*Digital Kyrgyzstan 2021*'

Organizing and conducting training courses and seminars for employees of the state bodies of the Kyrgyz Republic



MALAYSIA

CyberSecurity Malaysia

CyberSecurity Malaysia

Background

CyberSecurity Malaysia is the national cybersecurity specialist agency under the Ministry of Communications and Multimedia Malaysia. CyberSecurity Malaysia provides specialised cybersecurity services which among them are:

Cyber Security Emergency Services

- Security Incident Handling
- Digital Forensic

Security Quality Management Services

- Security Assurance
- Information Security Certification Body

Cyber Security Professional Development and Outreach

- Information Security Professional Development
- Outreach

Cyber Security Strategic Engagement and Research

- Government and International Engagement
- Strategic Research

Industry and Research Development

Establishment

CyberSecurity Malaysia was established with the formation of the Malaysia Computer Emergency Response Team (**MyCERT**) on 13 Jan 1997 under the Ministry of Science, Technology, and Innovation Malaysia. On 19 Oct 2019, CyberSecurity Malaysia was put under the purview of the Ministry of Communications and Multimedia Malaysia. As a technical specialist agency, CyberSecurity Malaysia is committed to provide a broad range of cybersecurity innovation-led services, programmes, and initiatives to strengthen Malaysia's self-reliance in the cyber space.

Specialised Services

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

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

CyberSecurity Malaysia's specialised cybersecurity services are as follows:

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

Constituency

CyberSecurity Malaysia's constituency is the Internet users in Malaysia. Cybersecurity incidents within Malaysia that are reported either by the Malaysian or international public and organisations will be resolved by assisting the complainants with the technical matters. If an incident involves international cooperation, CyberSecurity Malaysia will request trusted parties in the country or constituency, where the incident originates, to assist in resolving the issues based on the common international collaborative platforms and agreement.

2020 Highlights

Participated in the APCERT Drill 2020 - *11 Mar 2020*

Participated in online training on Android Mobile Malware Case Study During Covid19 Lockdown, hosted by APCERT and Pacific Cybersecurity Operational Network (**PaCSON**) - *19 Aug 2020*

Participated and co-organised the OIC-CERT Cyber Drill with Oman National CERT. The theme was '*Remote Working and Cyber Threats*' - *22 Sep 2020*

Participated in the Online APCERT Annual General Meeting (**AGM**) - *29 Oct 2020*

Participated in the Online 32nd Annual FIRST Conference - *16 to 18 Nov 2020*

Organised the Online OIC-CERT 12th Annual Conference 2020 with the theme '*Cyber Security Strategies & Practices During COVID-19 Crisis*' - *23 & 24 Nov 2020*

Participated in the China Computer Emergency Response Team (**CNCERT**) Online International Partnership in Emergency Response Conference - *16 Dec 2020*

Activities & Operations

Incident Handling Reports and Abuse Statistics

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

Android Mobile Malware Case Study During COVID19 Lockdown Online Training for APCERT-PACSON

CyberSecurity Malaysia had proactively produced 13 advisories and 18 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 2020

Most of the incidents reported were related to fraud and followed by intrusion as shown by the following graph.

Cyber Threat Research Centre

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

Other activities at 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

#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Spam	11	27	14	8	13	8	6	7	8	16	16	11	145
Intrusion Attempt	13	8	8	11	4	1	2	4	20	14	17	14	116
Denial of Service	0	1	3	7	1	0	0	1	0	2	1	0	16
Fraud	807	725	798	1,180	770	626	413	378	351	411	526	608	7,593
Cyber Harassment	37	27	58	65	73	69	48	32	40	50	60	37	596
Vulnerabilities Report	5	7	10	10	7	11	18	9	18	10	5	7	117
Malicious Codes	56	32	33	40	35	36	47	72	76	75	40	51	593
Content Related	23	23	42	23	9	7	7	6	7	11	7	5	170
Intrusion	122	93	125	144	133	113	101	102	81	87	88	255	1,444
	1,074	943	1,091	1,488	1,045	871	642	611	601	676	760	988	10,790

Lebahnet Project

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

The URLs of the Lebahnet project are:

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

Kibana portal at *https://es.honeynet.org.my/app/canvas#/workpad/workpad-7802f4ef-34aa-4690-8165-3921160bd371/page/1* by using guest authentication;
Username: guest
Password: guest2021!

Events organized by the organization / agency

Online Trainings

CyberSecurity Malaysia organized several online trainings as follows:

- Cloud and Smart Card Security: A Sneak Peak - *3 Mar 2020*
- WFH: Online Meeting Platform Security Demystified - *5 May 2020*
- Cybersecurity Awareness for All Users – *20 May 2020*
- Work from Home 2020 – *25 Jun 2020*
- Cybersecurity Technology - *13 Jul 2020*
- Mobile Incident Response and Digital Forensic - *29, 30 Jun & 8 Jul 2020*
- Certified Secure Application Professional (**CSAP**) – *2 to 5 Nov 2020*
- Digital Forensic Essential – *5 & 6 Nov 2020*
- Certified Information Security Awareness Manager (**CISAM**) – 10 &11 Nov 2020
- CSAP – *16 to 19 Nov 2020*
- Certified Penetration Tester (**CPT**) – *23 to 27 Nov 2020*
- Global ACE Certification Webinar - *25 Nov 2020*
- Cyber Security Awareness and Risk Governance for CxO & Board Members - *2 Dec 2020*
- Malaysia Common Criteria 2.0 (**MyCC**): Foundation Evaluator – *8 to 10 Dec 2020*

Online OIC-CERT 12th Annual Conference 2020

Due to COVID-19 pandemic, 2020 annual event was conducted virtually via the YouTube Live from 23 to 25 Nov 2020. Malaysia as the OIC-CERT Permanent Secretariat took the initiative to host the event. During the event, 12 papers were presented and viewed by 522 viewers on 23 Nov 2020, 643 viewers on 24 Nov 2020 and 1164 views on 25 Nov 2020.

CyberSecurity Malaysia CEO received Champion Award of the WSIS Prizes under Category 5 – Action Line C5: 'Building Confidence and Security in Use of ICTs' from Mr. Houlin Zhao, the ITU Secretary-General

Group photo with Communications and Multimedia Minister YB Dato' Saifuddin Abdullah as WSIS

Events Involvement

CyberSecurity Malaysia actively participated in cybersecurity events such as trainings, seminars, conferences, and meetings. The agency has contributed competencies in these activities.

Social Media

In 2020, CyberSecurity Malaysia received continuous invitations to speak about cybersecurity at the local radio and television stations. CyberSecurity Malaysia also

actively disseminates cybersecurity concerns through social media such as Facebook and Twitter. The Facebook Page has about 54,057 likes and the Twitter has 5,833 followers.

Memorandum of Understandings

CyberSecurity Malaysia has signed MoUs with the following organisations:

Backbone Connectivity Networks (Nigeria) Limited, Nigeria

The State Cybersecurity Service at the "Türkmenaragatnaşyk" Agency, Turkmenistan

International Roles

Amongst the roles and contributions by CyberSecurity Malaysia in the international arena are:

The Permanent Secretariat of the OIC-CERT, CyberSecurity Malaysia is facilitating cooperation and interaction among the members countries

The Chair of the APCERT

The Convenor for the APCERT Malware Mitigation Working Group – addressing malware infection among Internet users and cyber threat general issues. The main objectives are to provide an overview of cyber threats landscape by doing collaborative research to mitigate the cyber threats and sharing regular reports or data on malware attacks and focus on the impact analysis and remedial action

Cyber Drills

CyberSecurity Malaysia participated in two (2) international Cyber Drills in 2020 namely the APCERT Drill and the OIC-CERT Drill.

As in the previous years, CyberSecurity Malaysia was involved in co-organising international cyber drills for the OIC-CERT. In 2020, Malaysia collaborated with Oman in organising the drill with the theme, '*Remote Working and Cyber Threats*'. The objective of these drills are to get realistic experience in anticipating and handling some incidents related incidences and analysis of malwares. Fifteen (15) countries participated in the drill including APCERT and Africa CERT members listed as follows.

OIC-CERT	APCERT	Africa CERT
BGD e-GOV CIRT (Bangladesh)	HKCERT (Hong Kong)	bjCSIRT (ANSSI-Bénin)
BruCERT (Brunei)	CERT-In (India)	TZ-CERT (Tanzania)
BSSN (Indonesia)	Sri Lanka CERT/CC (Sri Lanka)	
Eg-CERT (Egypt)	TWNCERT (Taiwan)	
CyberSecurity Malaysia (Malaysia)	VNCERT/CC (Vietnam)	
maCERT (Morocco)		
CS2 Limited (Nigeria		
NR3C (Pakistan)		
PISA-CERT (Pakistan)		
Q-CERT (Qatar)		
SA-CERT (Saudi Arabia)		
SudanCERT (Sudan)		
SomCERT (Somalia) Observer		
TunCERT (Tunisia)		
aeCERT (UAE)		
UzCERT (Uzbekistan)		

2020 Achievements

OIC-CERT Malware Research and Coordination Facility

This is a collaborative effort of the OIC-CERT, APCERT and other organisations from various countries. The project is an initiative by CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT. In 2020, 12 issues of the Malware Trend Report have been published. The reports can be viewed at *https://www.oic-cert.org/en/malwarereport.html*.

The Global ACE Certification Scheme as the WSIS Winner 2020

The Global ACE Certification Scheme project was named as one of the World Summit on Information Society Prizes (**WSIS Prizes**) 2020 Winner at the WSIS Forum 2020 in Geneva, Switzerland. The prize was conferred under Category 5 – Action Line C5: '*Building Confidence and Security in Use of ICTs*' in recognition to CyberSecurity Malaysia's initiative on a project entitled the '*Global Accredited Cybersecurity Education Scheme: Centre of Excellence for Capacity Building and Lifelong Learning*'.

The WSIS Forum 2020 is the world's largest ICT annual gathering of the '*ICT for development*' community hosted by the International Telecommunication Union (**ITU**), and co-organised by United Nations Educational, Scientific and Cultural Organization (**UNESCO**), United Nations Conference on Trade and Development (**UNCTAD**) and United Nations Development Programme (**UNDP**) in close collaboration with all WSIS Action Line Facilitators / Co-Facilitators.


WSIS PRIZES 2020 WINNER

WORLD SUMMIT ON THE INFORMATION SOCIETY

CERTIFICATE OF RECOGNITION

The International Telecommunication Union is proud to award

CyberSecurity Malaysia
Malaysia

Winner of WSIS Prizes 2020
Category 5
Building confidence and security in the use of ICTs

for its outstanding contribution towards strengthening the implementation of the World Summit on the Information Society (WSIS) Outcomes

Houlin Zhao
ITU Secretary-General

Geneva, 07 September 2020

Research Papers

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

- Mobile Malware Classification for Social Media Application - IEEE Xplore Digital Library
- Using Text Annotation Tool on Cyber Security News: A Review - IEEE Xplore Digital Library
- Method for Generating Test Data for Detecting SQL Injection Vulnerability in Web Application - IEEE Xplore Digital Library
- Ransomware Entities Classification with Supervised Learning for Information Text - IEEE Xplore Digital Library
- Feature Extraction and Selection Method of Cyber Attacks and Threat Profiling in Cybersecurity Audit - IEEE Xplore Digital Library
- TAGraph Knowledge Graph of Threat Actor - IEEE Xplore Digital Library
- OTPAF: A Security Requirement Conceptual Model of Cloud SaaS for Malaysian Government Based on Common Criteria - IEEE Xplore Digital Library
- Cloud Service Provider Security Readiness Model: The Malaysian Perspective - IEEE Xplore Digital Library

An Attribution of Cyberattack using Association Rule Mining (ARM) - The Science and Information Organisation

A Malware Detection Framework Based on Forensic and Unsupervised Machine Learning Methodologies - ACM Digital Library

Cryptojacking Classification Based on Machine Learning Algorithm - ACM Digital Library

The Capabilities that Terrorist Possess in the Digital Age - Özgür Öztürk Dakam Yayinlari

S-Box Construction Based on Linear Fractional Transformation and Permutation Function - MDPI

Secure Information Hiding Based on Random Similar Bit Mapping - International Association of Computer Science and Information Technology

Slid Pairs of the Fruit-80 Stream Cipher - Institute of Information Technology

Mitigating Insider Threats: A Case Study for Data Leakage Prevention - Academic Conferences and Publishing International Limited

OS Kernel Malware Detection through Data Characterization of Memory Analysis - Academic Conferences and Publishing International Limited

A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Dataset, Open Challenges and Recommendations - MDPI

Fraudulent e-Commerce Website Detection Model Using HTML, Text and Image Features - Springerlink

Malware Behavior Profiling from Unstructured Data - Springerlink

Findings Annihilator(s) via Fault Injection Analysis (FIA) on Boolean Function of LILI-128 - Engineering and Technology Publishing

Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT - IEEE Xplore Digital Library

Randomness Analysis on Lightweight Block Cipher, PRESENT - Science Publications

2021 Planned Activities

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

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

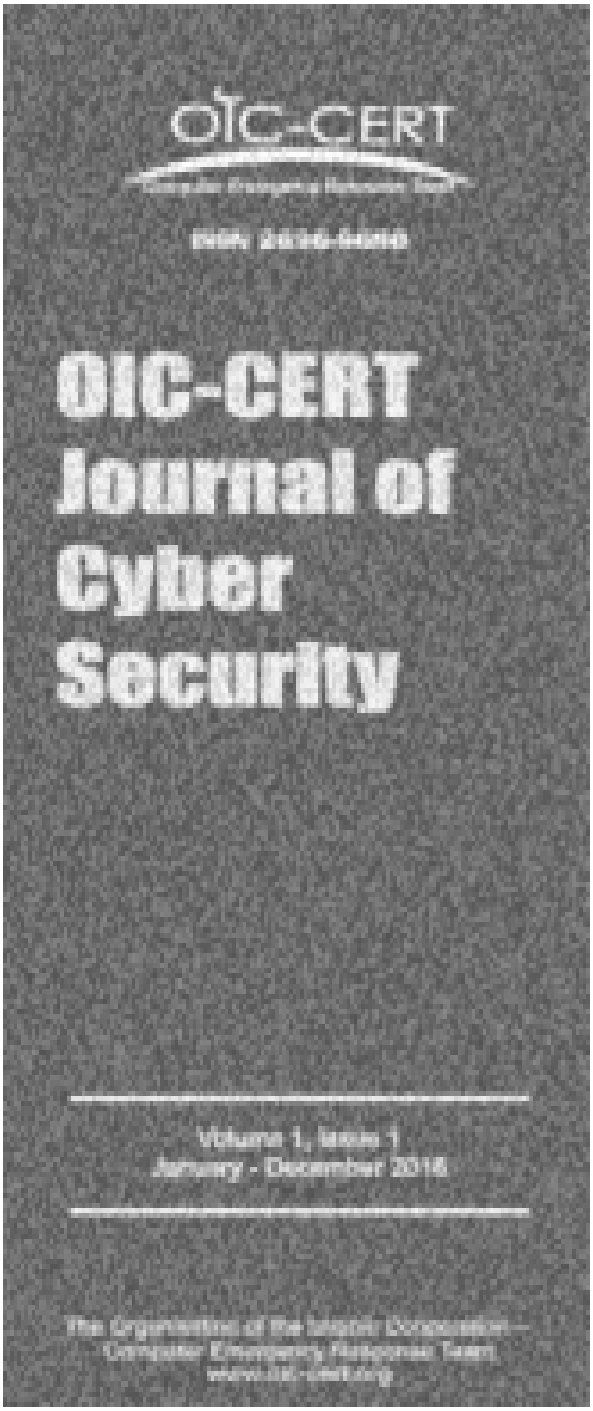
Since the Covid 19 pandemic outbreak, CyberSecurity Malaysia has postponed several national events such as the CyberSecurity Malaysia – Awards, Conference and Exhibition (**CSM-ACE**) and the National ICT Security Discourse. The agency will continue with these events when the Covid 19 situation makes it possible in the future. At the international arena, CyberSecurity Malaysia, as the Permanent Secretariat of the OIC-CERT, will spearhead the collaboration and organise international events such as the OIC-CERT Annual Conferences.

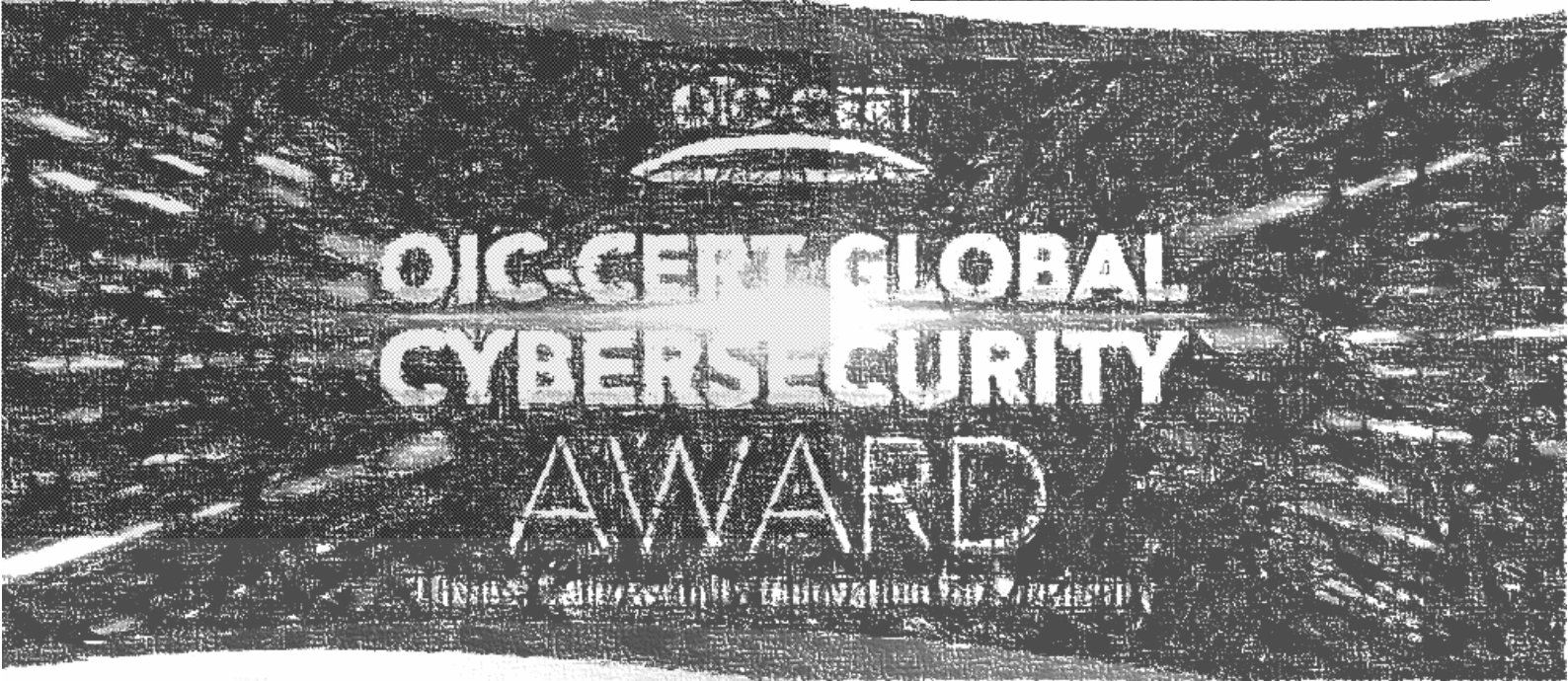
With such understanding, CyberSecurity Malaysia supports newly established local and international CSIRT by providing advice and assistance especially in becoming members to international security community such as the APCERT, FIRST and OIC-CERT.

CyberSecurity Malaysia as the OIC-CERT Permanent Secretariat hosted the OIC-CERT 12th Annual Conference (Virtual) – 23 to 24 Nov 2020

Deputy Communications and Multimedia Minister Datuk Zahidi Zainul Abidin officiated the OIC-CERT 12th Annual Conference (Virtual) - 23 Nov 2020

Moderator and speakers presented their papers for Session 1 of the OIC-CERT 12th Annual Conference (Virtual)





NIGERIA

Consultancy Support Services Limited

Consultancy Support Services Limited

(**CS2**)

Background

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

Establishment

CS2 was incorporated on 13 Feb 2002.

Resources

Cybersecurity Specialist

Library and Information Management Specialist

Information Management and Systems Networking

Computer Programming and Enterprising Management

Digitization, Archiving and Digital Libraries

Computer Forensics and Cybersecurity

Digital Library

IT Infrastructure.

Constituency

The public and private sectors as well as academia, media, and non-governmental organisations in Nigeria, Africa, and across the globe.

2020 Highlights

Summary of Major Activities

Successfully chaired the Review of National Cybersecurity Policy and Strategy

Initiated the OIC-CERT Global Cybersecurity Award

Carried out a diagnostic Assessment of Galaxy Backbone Limited (**GBBL**) 2020

Cybersecurity assessment for the Nigeria Identification for Development Project for the National Identification Management Commission (**NIMC)** 2020

APCERT Cyber Drill 2020

Defence Space Administration (**DSA**) CERT 2020

The 8th Arab Regional and OIC CERT Cyber Drill 2020

Achievements

Successfully chaired the Review of National Cybersecurity Policy and Strategy for the Office of the National Security Adviser (**ONSA**) and approved by the President of Nigeria

Initiated the OIC-CERT Global Cybersecurity Award, which has been approved by the OIC-CERT Board

Carried out a diagnostic assessment of GBBL, an ICT services provider, wholly owned company by the Federal Government of Nigeria

Successfully completed a cybersecurity assessment of the Nigeria Identification for Development Project for the National Identification Management Commission - *2020*

Supported the Department of Cybersecurity of the Federal University of Technology (**FUT**), Minna, Nigeria. The institution is obtaining re-accreditation for the department and its cyber-forensics teaching, learning and research activities

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

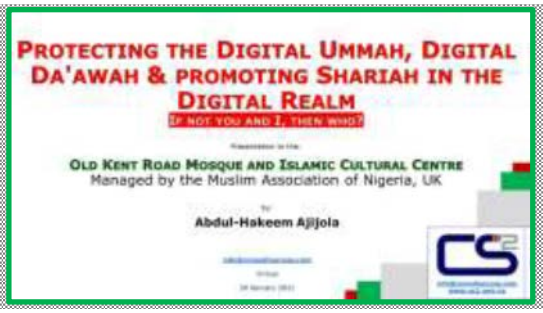
Honoured with the Fellowship Award from NCS

Participated in the cyber drills:

- APCERT Cyber Drill 2020
- DSA CERT 2020
- The 8th Arab Regional and OIC-CERT Cyber Drill 2020

Facilitated training activities including:

- A presentation titled '*Protecting the Digital Ummah, Digital Da'awah & promoting Shariah in the Digital Realm: If not you and I, then who?*' at the Old Kent Road Mosque and Islamic Cultural Centre, London, United Kingdom (**UK**). A similarly title intervention was made at the Great Heights Academy (Girls High School) in Kado, Abuja, Nigeria



- Executive Registration Programme (**ERP**) for the Computer Professionals Registration Council of Nigeria (**CPrN**) - *2020*
- Mandatory Continuing Professionals Development (**MCPD**) of CPrN for the National Insurance Commission (**NAICOM**) - *Sep 2020*
- Organised the National Cybersecurity Competition '*HackXploit*' in collaboration with the FUT Minna, and Centre for Cyberspace Studies, Nasarawa State University, Keffi (**NSUK**) with top-level participants being offered employment in the national selected security entities

Brokered MoU and bilateral agreements between Backbone Connectivity Network Nigeria Limited and:

- Vigilant Asia - a managed security service provider, and a wholly own subsidiary of Efficient E-Solutions Berhad
- Cybersecurity Malaysia - an agency under the Ministry of Communications and Multimedia Malaysia

Participants Group Photograph at APCERT Drill 2020

CS2 Training session during CPrn ERP Training, March 2020

Group photograph with participants at Leadership & ICT Training at CentreLSD

Plaque being presented to the Chief Executive Officer of CS2 after a successful speech to the Excursion students of FUT, Minna

Participants during the 2020 OIC CERT Cyber drill

Activities & Operations

Events organized by the organization / agency

Hands on exhibition of forensic equipment to cybersecurity students at FUT Minna

Events involvement

OIC-CERT Cyber Drill 2020

APCERT Cyber Drill 2020

Cybersecurity meeting for NCS – *08 Jan 2020*

National Broadband Plenary - *21 Jan 2020*

Speaker at the Pan-African Cyber Law Summit Plenary, Pretoria, South Africa – *02 to 04 Mar 2020*

Global Forum on Cyber Expertise (**GFCE**) Workshop on Critical Information Infrastructure Protection (**CIIP**), Dakar, Senegal – *05 Mar 2020*

Executive Registration Programme for CPrN - *21 Feb 2020*

AU – African Union Cybersecurity Expert Group (**AUCSEG**), Addis-Ababa – *17 and 18 Mar 2020*

DSA First Quarter CERT Drill – *26 Mar 2020*

GFCE 5th Anniversary Conference - *14 to 16 Apr 2020*

GFCE Cyber Capacity Assessment - *28 Apr 2020*

Facilitated the Executive Registration Programme of CPrN for Shell Nigeria – *09 May 2020*

Facilitated the virtual training on Cybersecurity in Digital Economy, to staff and students at the Nile University of Nigeria - *21 May 2020*

Discussion on "*COVID-19: Working from home presents new cybersecurity challenges for firms*" at CNBC Africa - *May 2021*

Dialogue on the gains of virtual engagements during the pandemic at the Nigerian Television Authority (**NTA**) - *18 Jun 2020*

Participate in the Digital African Conference & Exhibition – *23 to 25 Jun 2020*

Facilitated the CPrN MCPD for NAICOM - *18 Sep 2020*

Participated as a panellist in '*Are Cyber Norms Equivalent International Law in Cyber Space*' – *24 Sep 2020*

Speaker – CyFy: '*The Return of the Sovereign: Drawing Boundaries in Cyber Space*' – *12 – 16 Oct 2020*

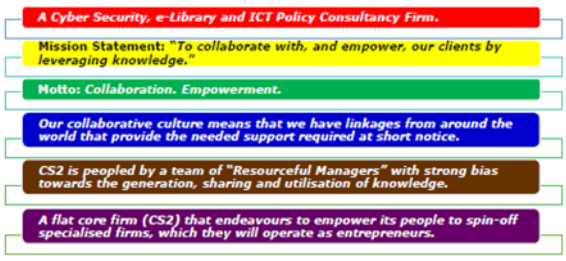
Chaired the review Committee of the National Cybersecurity Policy and Strategy Review - *21 Oct 2020*

Served as a judge at the Future Hack Cybersecurity Competition in Port Harcourt, Nigeria

Participated in the National Information Technology Development Agency (**NITDA**) for Exploring Cybersecurity Opportunities in the Digital Economy – *22 Oct 2020*

Panel discussion at the Internet Governance Forum (**IGF**) 2020 on Trust & Confidence Building Mechanisms (**CBM**) in cyberspace in the context of Africa - *12 Nov 2020*

Facilitated training on '*Leadership & ICT on Cybersecurity*' for the African Centre for Leadership, Strategy & Development (**CentreLSD**) & Konrad Adenauer-Stiftung - *05 Dec 2020*



Facilitated the Executive Registration Programme of CPrN – *16 Dec 2020*

2021 Planned Activities

Profile Summary

Support the Government of Liberia in the development of their National Cybersecurity Policy, Strategy, and related initiatives

Increased involvement in the OIC-CERT, GFCE, AUCSEG, Global Commission on the Stability of Cyberspace (**GCSC**), Global Accredited Cybersecurity Education (**GlobalACE**) Certification, Internet Corporation for Assigned Names and Numbers (**ICANN**), NCS, CPrN, Cyber Security EXPERTS Association of Nigeria (**CSEAN**), and related activities

Implement the in-house a cyber forensics capacity development program

Kickstart the development of Podcast and Vodcast initiatives

Implement Online testing and certification facilities for GlobalACE Certification

Develop the multimedia content including tutorials for eLibraries

Provide services in support of the military-civilian, law enforcement and related cybersecurity initiatives

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

Support the following national initiatives:

- Implementation of the Nigeria National Broadband Plan
- Implementation of the Nigeria of the National Cybersecurity Strategy
- Implementation of the Nigeria ICT Roadmap
- Harmonisation, standardisation, and seamless interoperability of the national identity systems as well as evolving a Business Model / Plan defining the rules of engagement governing access of Foundation Identity by the agencies / organisations providing the functional national identity

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

Implementation of a Nigeria 'e-Trustmark' to validate the e-Business activities, website security, applications, hardware, software, legality, and good 'e-Business' behaviour

Establishment of a cadre of Information Security Professionals with direct reporting line to the Chief Executive of their assigned

ministry, department, and agency (**MDA**) as well as the Office of Head of Information Security for the Nation at NITDA

Establishment of a local Cybersecurity Certification Authority with International credibility to increase the number of cybersecurity professional by leveraging on the Global ACE Scheme and other partnerships

Develop the digital literacy and e-inclusion schemes for under-served communities including women and girls

Increase the compliance and adoption of IPv6 standards

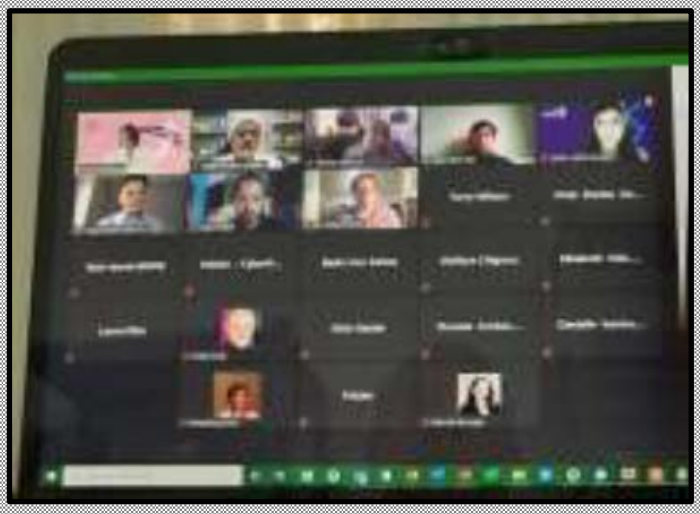
Strengthening of ICT departments in the Higher Education Institutions (**HEI**s)

Development of a blueprint of common services, policies, standards, procedures, and technical components that guide the MDAs on IT investment

Participants Group Photograph at OIC-CERT Cyber Drill 2020

CS2 Training Session in collaboration with CPrN & NAICOM

Leadership & ICT Training at CentreLSD



Session during GFCE Anniversary Conference 2020

IGF2020 Panel Session

Hack Cybersecurity Competition, Port Harcourt

OMAN

Oman National Computer Emergency Readiness Team

Oman National Computer Emergency Readiness Team (OCERT)

Background

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

Resources

CNII Protection team

Cybersecurity Training and Awareness team

Threat and Risk Management team

Incident Response team

Vulnerability Assessment and Penetration Test team

Digital Forensics team

Alliances and Cooperation team

ITU-Arab Regional Cyber Security Centre team

2020 Highlights

Summary of Major Activities

2020 Achievements

Regional and International

ITU Arab Regional Cybersecurity Centre (**ITU-ARCC**) participated as Supporting partner in the 5th GCC Operational Technology Security Forum which was held in Muscat - *1 to 4 Mar 2020*

The Sultanate chaired the (OIC-CERT) 12th Annual Conference 2020

The "5th GCC Operational Technology Security Forum and Industrial CyberSecurity Workshop" – 1 to 4 Mar 2020 in Oman

ITU-ARCC organized the Regional Cybersecurity Awareness campaign for one month - Apr 2020. The campaign was targeting regional and international participants to raise the cybersecurity awareness during the COVID 19 pandemic. The campaign covered the following four topics:

- Week 1 (5-8 April) : Remote Working
- Week2 (12-16 April): Remote Education
- Week3 (19-23 April): Blackmailing in Corona
- Week4 (26- 30 April): Cybersecurity Recommendations after Corona

There were participations from 7 countries: (Kingdom of Saudi Arabia (**KSA**), Qatar, Tunis, Egypt, Syria, Oman, Lebanon) on sharing different awareness materials with different languages, in cooperation with 2 strategic partners (Silensec & Kaspersky) and a researcher (Mohamed Maaz, Google fellow) which have successfully raised the awareness using online platforms to reach all targets and audiences

ITU-ARCC organized in partnership with Humanitarian Dialogue (**HD**) Centre a proactive measurements concept paper to the Arab region

Conducted Oman National Threat hunter awarding ceremony - *25 Jul 2020*

Conducted the National Cyberstars Competition 2020 with a participation from 10 countries (Oman, Kuwait, Qatar, Syria, Tunisia, Palestine, Sudan, Lebanon, Egypt and Morocco) and over 1,000 contestants

Conducted the 8th Arab Regional and OIC-CERT Cyber Drill 2020 virtually. The cyber drill was under the theme '*Remote Working and Cyber Threats*' with participation of 25 teams from 24 countries – *22 Sep 2020*

Conducted the Final Arab Regional Threat Hunters, 3rd Edition - *26 Sep 2020*

Participated in the Organization of the Global Cyber Drill 2020 with the first cybersecurity scenario - *27 Oct 2020*

Organized and managed HD virtual workshop titled '*Protecting Critical Information Infrastructure*' - *26 Oct 2020*

ARCC participated in a video in the ITU Arab Regional Development Forum - *25 to 26 Nov 2020*

Final Arab Regional Threat Hunters - 3rd Edition on 26th Sep 2020

ITU-ARCC organized the Regional Cybersecurity Awareness campaign for one month - April 2020. Week1 - Remote Working

Promoting and supporting Women in Cyber Security Middle East (**WiCSME**) 1st virtual conference - *14 Nov 2020*

ITU-ARCC celebrated the Safer Internet Day (SID2020) with participation from the regions (Lebanon, Tunisia, and Syria) - *11 Feb 2020*

Chaired the OIC-CERT 12th Annual Conference - *23 and 24 Nov 2020*

Participated in the Regional Remote Dialogue on Guiding Principles for '*Online Child Protection on the Internet*' with ITU - *23 Nov 2020*

Cybersecurity Cooperation and Alliances

ITU-ARCC have established a cybersecurity cooperation partnership with the Humanitarian Dialogue (**HD**) Centre in Geneva

Cooperated with HD centre to conduct a workshop for certain Arab countries as member of OIC-CERT and further cooperation with OIC-CERT members

Evaluation of the OIC-CERT signed MoUs with counterparts and cybersecurity organizations, and engaged FIRST to contribute and bringing speakers in the in 12th OIC-CERT conference as part of MoU cooperation - *23 and 24 Nov 2020*

Developed with Saudi CERT the cybersecurity survey to study the implication of Covid-19 for Arab countries and to support the G20 Summit in KSA

Developed the '*OIC-CERT Social Media Guidelines*' to be used in OIC-CERT organization and helping them in the implementation of social media to market and promote OIC-CERT initiatives

Developed GCC-CERT Cooperation Framework

Activities & Operations

Cyber Incident and Services Management

Discovered and handled 417,021 real attempted service attacks, (55,338 web attacks, 82 malware attacks, 38,492 mobile attack and 4,034,570 phishing attacks) through OCERT Intelligence gathering System resulted from the analysis of millions of attempted attacks against the Oman cyber-space

Successfully and comprehensively handled 1,461 real cybersecurity incidents reported by the government, CNIIs and public

Published 107 Security Threat Notification and Alerts "TNAS" on cybersecurity threats to OCERT constituents

Handled 128 digital forensics cases with 671 evidence devices including computers, mobile, phones, external hard disk and USBs resulted from cybercrime cases in Oman

Cyber Security Professional Services

Organized the National Cyber Drill for Government entities with participation from 31 organizations

Cybersecurity Ambassador Program

- Cybersecurity ambassadors have participated in 'threat hunter' competition organized by OCERT
- 966 new cybersecurity ambassadors joined the OCERT ambassador program bringing the total of cybersecurity ambassadors to 1749

Unified Government Information Security Campaign 'WAAY'

- 12 online Awareness sessions for government entities attended by more than 750 people
- 1 awareness session presented to Oman Royal Force and attended by 70 people

Child Online Protection (**COP**)

- Participated in ITA kids event
- Conducted 5 online awareness sessions on COP

Awareness during Covid 19

- Developed 6 awareness posters
- Participated in 11 Radio Interviews
- Participated in 2 TV Interviews

Others

- Participated in 5th edition of GCC Operational Technology Security Forum
- Organized Oman participation in Safer Internet day
- Participated in MTC Cyber Talk
- Participated in smart cities forum and events

ITU-ARCC organized the Regional Cybersecurity Awareness campaign for one month - April 2020. Week1 - Remote Working

ITU-ARCC organized the Regional Cybersecurity Awareness campaign for one month - April 2020. Week2 - Remote Education

ITU-ARCC organized the Regional Cybersecurity Awareness campaign for one month - April 2020. Week3 - Blackmailing in Corona

ITU-ARCC organized the Regional Cybersecurity Awareness campaign for one month - April 2020. Week4 - Cybersecurity Recommendations after Corona

The 8th Arab Regional & OIC-CERT Cyber Drill 2020 virtually on 22nd Sep 2020

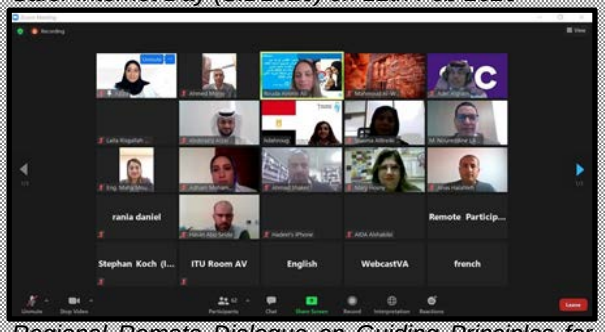
Oman National Threat hunter awarding ceremony on 25th Jul 2020

Oman National Threat hunter awarding ceremony on 25th Jul 2020

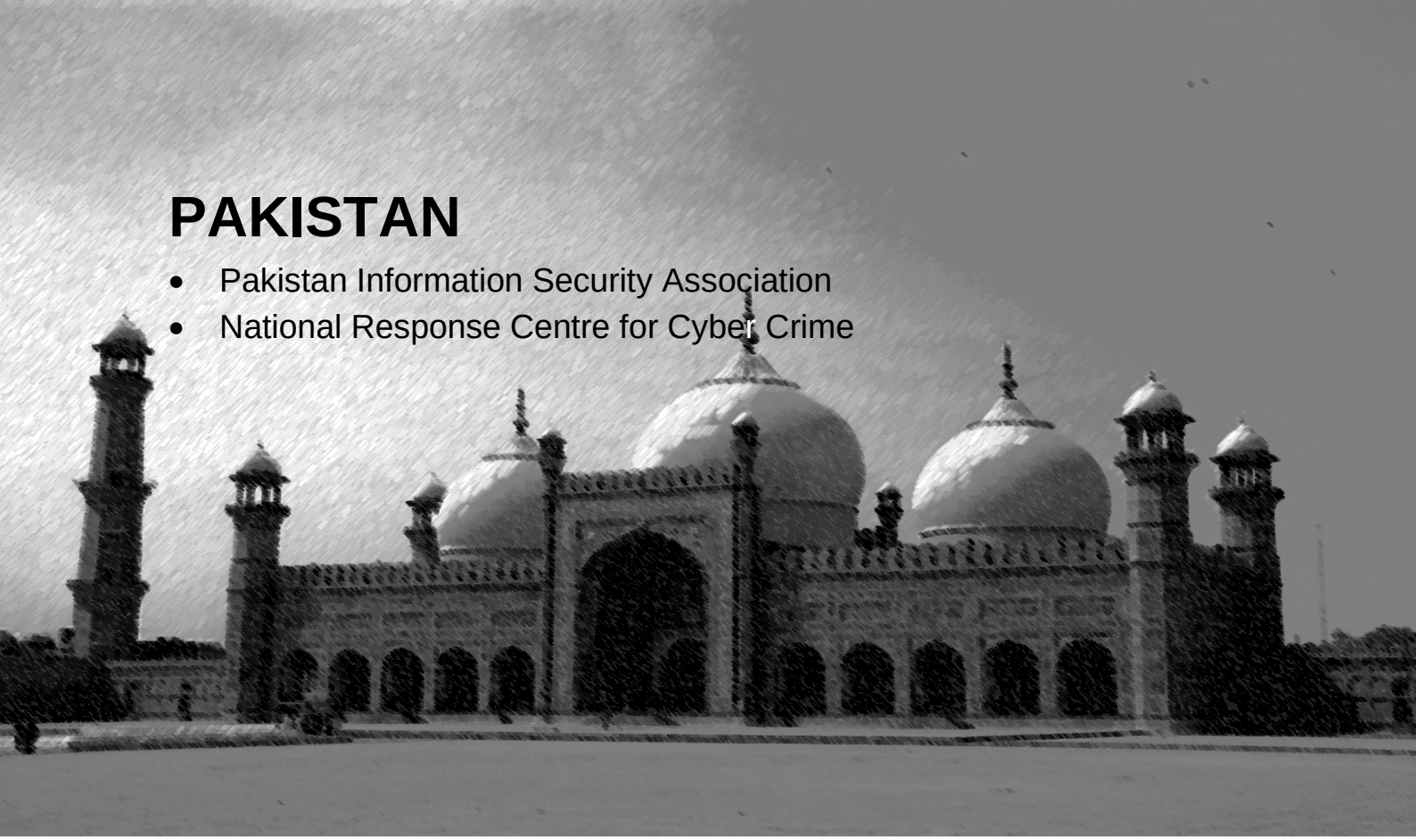
The Organization of the Global Cyber Drill 2020 with the first cyber security scenario conducted on 27th Oct 2020

Women in Cyber Security Middle East WiCSME 1st virtual conference on 14th November 2020

Safer Internet Day (SID2020) on 11th Feb 2020



Regional Remote Dialogue on Guiding Principles for "Online Child Protection on the Internet" with ITU on 23rd November 2020



PAKISTAN

- Pakistan Information Security Association
- National Response Centre for Cyber Crime

Pakistan Information Security Association (PISA)

Background

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

Establishment

PISA was established in 2005.

Constituency

Pakistan

2020 Highlights

Summary of Major Activities

Cyber Security Changing Paradigm, Artificial Intelligence for National Security in Hybrid Warfare – *2 Jan 2020*

National Seminar Artificial Intelligence; Implication on National Security – *28 Jan 2020*

Tracking the Criminals in Cyber Space for Law Enforcement – *22 Feb 2020*

Participated in APCERT Cyber Drill – *11 Mar 2020*

Business Continuity Planning during and after Corona – *29 Mar 2020*

Cyber Security for corporate and enterprise during '*Work from Home*' – *5 Apr 2020*

Cybersecurity and Role of ISPs, Telecoms, and Regulators in the Current Pandemic Situation – *12 April 2020*

Cybersecurity and Challenges to the Health Care in Institutions in the Current Pandemic Situation – *19 Apr 2020*

Threat Spectrum of Cyber Terrorism and Sabotage in South Asia '*Challenges and Opportunities for Pakistan*' – *18 May 2020*

CyberXchange Live Online Summit – *28 & 29 May 2020*

High-level dialogue to discuss the Information Security Laws / Framework for Cyber Secure Pakistan – *7 June 2020*

International CyberEx 2020 Capture the Flag Competition – *10 Sep 2020*

Participated in OIC-CERT Cyber Drill – *22 Sep 2020*

Role of Women in digital Transformation of developing Countries Challenges and Opportunities – *12 Nov 2020*

Workshop on Cyber Security for NextGen – *18 Oct 2020*

Cyber Threat Intelligence 2020, 3rd International Conference – *19 Nov 2020*

OIC-CERT 12th Annual Conference 2020 – *24 Nov 2020*

Paris Blockchain Summit – Live Event – *9 Dec 2020*

Online Conference on CNCERT International Partnership in Emergency Response – *16 Dec 2020*

2020 Achievements

In 2020 PISA has completed the following target.

- Participated in International Cyber Drills
- Conducted Seminars / Workshops on Cyber Security
- Participated in the national and international competition (CTF / CyberLympics)

Several students and professionals (universities and law enforcement) have been trained in Cybersecurity and Information Security by PISA.

Activities & Operations

Events organized by the organization / agency

Tracking Criminals in Cyber Space for Law Enforcement

Business Continuity Planning during and after Corona

Cybersecurity for Corporate and Enterprise during "*Work from Home*"

Cybersecurity and Roles of ISPs, Telecoms, and Regulators in the current pandemic situation

Cybersecurity and Challenges to Health Care in Institutions in the current pandemic situation

High level dialogue to discuss the Information Security Laws / Framework for Cyber Secure Pakistan

Role of Women in Digital Transformation for Developing Countries - Challenges and Opportunities

Workshop on Cyber Security for NextGen

Events involvement

Cyber Security Changing Paradigm, Artificial Intelligence for National Security in Hybrid Warfare

National Seminar Artificial Intelligence - Implication on National Security

Participated in APCERT Cyber Drill

CyberXchange Live Online Summit

Participated in the International CyberEx 2020 Capture the Flag Competition

Participated in the OIC-CERT Cyber Drill

Represent Pakistan in OIC-CERT 12th Annual Conference 2020

Supported in 3rd International Conference, Cyber Threat Intelligence 2020

Online Conference on CNCERT International Partnership in Emergency Response

Paris Blockchain Summit – Live Event

Achievement

In 2020 PISA has achieved all targets set in 2019. Participated in International Cyber Drills and successfully organized seminars, 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

2021 Planned Activities

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

Planned to organize the mega event on Cybersecurity on the 21st Century Silk Road (Belt & Silk Road Initiative)

Planned to organize in-house Cyber Security Drills

Planned to Participate in International Cyber Security Drills, Capture the Flag (**CTF**) competition, CyberLympics

Planned to Organize Cyber Security/Information Security Seminar, workshops for universities, Government, and Private sector

Inter

Cyber Threat Intelligence Annual Conference 2020

OIC-CERT Cyber Drill 2020

National Response Centre for Cyber Crime (NR3C)

Background

NR3C has expertise in Digital Forensics, Technical Investigations, Information System Security Audits, Penetration Testings, and Trainings. The unit since its inception has been involved in capacity building of the officers of Police, Intelligence, Judiciary, Prosecutors, and other Govt. organizations. NR3C has also conducted many seminars, workshops and training / awareness programs for the academia, print / electronic media, and lawyers. Cyber Scouts is the latest initiative of NR3C, in which, selected students of different private / public schools are trained to deal with computer emergencies and spreading awareness amongst their fellow students, teachers, and parents. The NR3C which stands for the National Response Centre for Cyber Crime – Federal Investigation Agency (**FIA**) is a law enforcement agency dedicated to fighting cybercrimes. Inception of this Hi-Tech crime fighting unit transpired in 2007 to identify and curb the phenomenon of technological abuse in the society. The objectives of NR3C is the latest introduction to the mandate of the FIA primarily to deal with technology based crimes in Pakistan. It is the only unit of its kind in the country and in addition to the directly received complaints also assists other law enforcement agencies in their cases.

Statistics regarding cybersecurity and cybercrime complaints are as follows in year 2020.

Establishment

NR3C was established in 2007 as a Project

All officers and Man Power of NR3C was regularized in 2012

All officers inducted in phase-II of NR3C is in process of regularization (becoming permanent)

NR3C's inducted officers in Phase-III are serving as the employees of Project

Resources

NR3C is state run wing of FIA. Resources required to meet the organizational objectives are provided by the state. Resources allocated / allotted by the state are financially sponsored through Agency's Budget or through PSDP funded project. In either case NR3C is a state-run organization and the state of Pakistan allocate resources to meet organizational objectives. NR3C is state-run organization and represents the interests of the State of Pakistan at the

national Level. NR3C is a full member of OIC-CERT since its first seminar in 2009 in Kuala Lumpur, Malaysia. Therefore, the objectives of NR3C are aligned with the objectives of OIC-CERT. Total manpower of NR3C is four hundred and seventy-seven (477) well trained staff. Government of Pakistan has allocated budget of Rs. 3 billion rupees for NR3C in 2020.

Sr. No.	Organizer	Host	Topic	Date	Virtually Attended By
1	OIC-CERT	UAE	Remote Working Security	29th April 2020	Muhammad Akram, DD/NS NR3C/FIA
2	OIC-CERT	UAE	Social Engineering	18-May 2020	Muhammad Akram, DD/NS NR3C/FIA
3	OIC-CERT	UAE	Malware	04-June-2020	Muhammad Akram, DD/NS NR3C/FIA
4	OIC-CERT	Malaysia	Managing Technical Journal Online 4th Industrial Revolution	14-July-2020	Muhammad Akram, DD/NS NR3C/FIA
5	OIC-CERT	Indonesia	Managing Security Incident Response during Covid Outbreak: A Lesson Learned	3 Sep 2020	Muhammad Akram, DD/NS NR3C/FIA
6	OIC-CERT	UAE	Mobile Security	21 Sep 2020	Muhammad Akram, DD/NS NR3C/FIA
7	OIC-CERT	UAE	Social Media Security	18 November 2020	Muhammad Akram, DD/NS NR3C/FIA
8	OIC-CERT	UAE	Email Security	14-December 2020	Muhammad Akram, DD/NS NR3C/FIA

Constituency

Public, National, and International

2020 Highlights

Summary of Major Activities

NR3C contributed to the formulation of the National Internet & Email Policy. The said Policy is approved by the Honourable Prime Minister of Pakistan

NR3C contributed to the formulation of the National Information Technology Policy

NR3C participated and contributed to the National Cybersecurity Strategy. The said strategy is in the process of its formulation

NR3C pivotally participated in the formulation of Prevention of Electronic Crimes Act 2016 (**PECA 2016**) and subsequently rules

Officers of NR3C authored research paper on "*National Cybersecurity Policy in the context of South Asia*". The afore-mentioned paper was presented at the National Defence University Islamabad

NR3C initiated the Cybersecurity Legislation Process for enforcement in Pakistan

NR3C participated in a cybersecurity seminar organized by CECOS University Peshwar

NR3C participated or independently carried out the Information Security Audit of Multiple State institutions

Translated the *OIC-CERT Malware Trend Report H1 2020 v1* into layman language and distributed it amongst senior officers

NR3C contributed to the 5-year counter cyber terrorism strategy with the National Counter Terrorism Authority (**NACTA**)

Following Online Trainings were attended (virtually) by NR3C in 2020:

NR3C / FIA participated in the Cyber Security Drill 2020 and emerged amongst best 3 scorers. Result of Cybersecurity drill is attached herewith for ready reference and kind perusal

NR3C / FIA participated in OIC-CERT 12th Annual Conference (Virtually) in November 2020

Activities & Operations

Events organized by the organization / agency

Seminars in Karachi

Seminars in Islamabad

Seminars in Lahore

Events involvement

Participant in online trainings

Organizer of seminars in Karachi, Islamabad, and Lahore

Achievements

Prevention of the Electronic Crimes Act is enacted and thousands of people get relief annually. NR3C received 9108 complaints in

2020 in Gujranwala alone. Processing the received complaints revealed that 15.83% of the received complaints were regarding cybersecurity (Hacking) incidents in Pakistan

National Internet and Email Policy is approved and enforced nationwide

National Cybersecurity Strategy is in the process of discussion in the Senate of Pakistan and in the Ministry of IT and Telecom

National Cybersecurity Act is at the initial stages of discussion and expected to be approved in the next couple of years

NR3C initiated the Cyber Scouts Program and prepared students at schools and colleges for awareness regarding cybercrimes and cybersecurity

12, 458 individuals from all walks of life have been trained by NR3C to serve the purpose of cybercrime mitigation and cybersecurity implementation

NR3C Initiated Cyber Alert Service. The said Service over mobile phones generated alerts in the form of messages regarding cybersecurity incidents which resulted in reducing cybercrimes. This is an effort to spread public awareness regarding cybercrimes and cybersecurity incidents via SMS

2021 Planned Activities

Training Plan for the Police Officers

Training Plan for the Academia

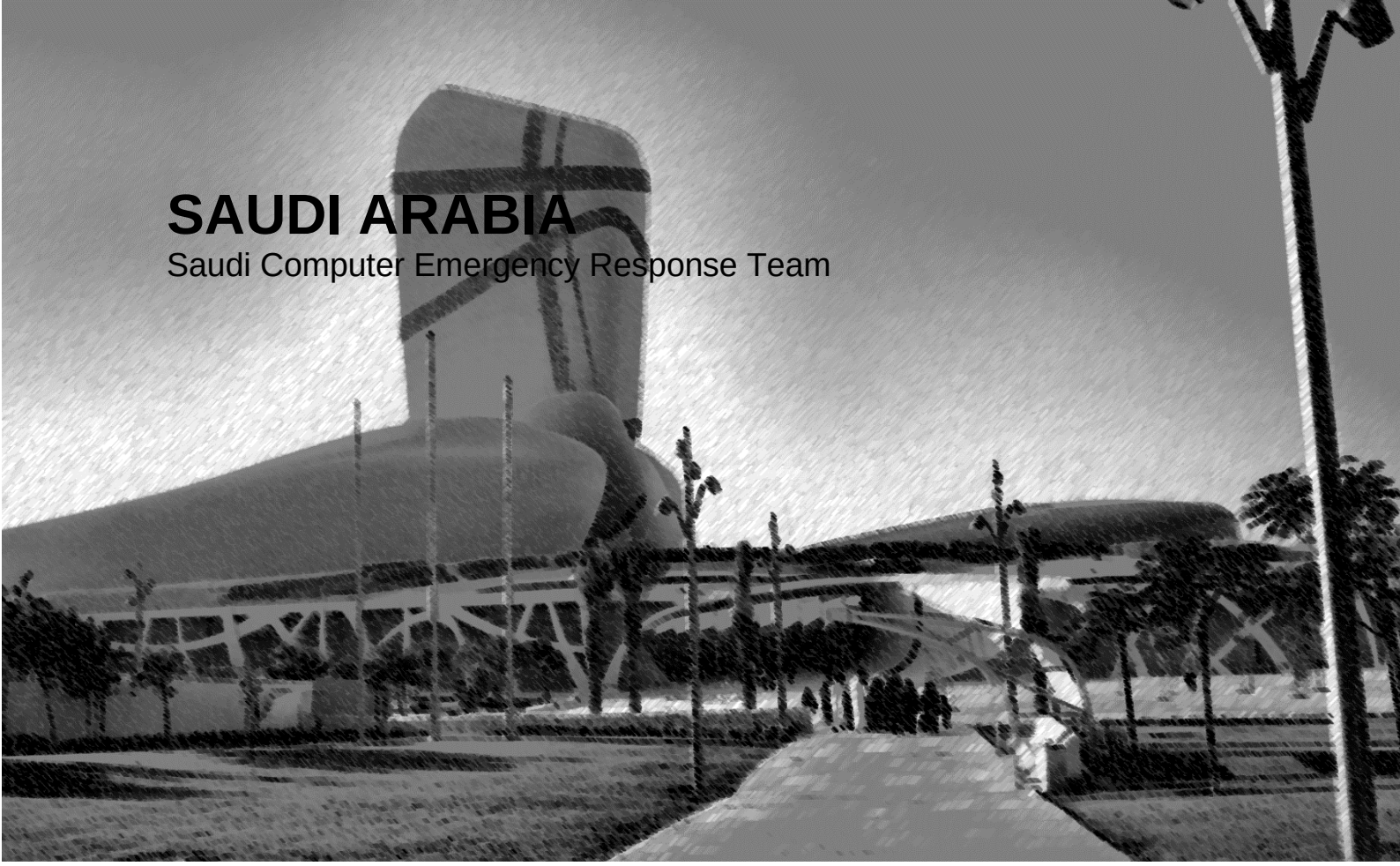
Training Plan for the Industry

To attend all online trainings organized by the OIC-CERT

To participate in Cybersecurity Drill of the OIC-CERT

To attend the OIC-CERT Annual Conference

To submit research papers for publication in the OIC-CERT Journal of Cybersecurity



SAUDI ARABIA

Saudi Computer Emergency Response Team

Saudi Computer Emergency Response Team (SAUDI CERT)

Background

Saudi CERT's primary mission is to raise cybersecurity awareness in the Kingdom of Saudi Arabia. Saudi CERT increases the level of knowledge and awareness regarding cybersecurity risks and attempts to mitigate their impact by issuing warnings about the latest and most dangerous vulnerabilities. Saudi CERT has also launched awareness programs and campaigns and cooperates and collaborates with other response teams.

Establishment

The National Cybersecurity Authority (**NCA**) was established by a Royal Decree on 11/2/1439 to protect the Kingdom's vital interests, its national security, its critical infrastructure, priority sectors, government services and activities.

2020 Highlights

Summary of Major Activities

Launched cert.gov.sa as national portal for cybersecurity content and services that targets individuals

Launched multiple cybersecurity awareness campaigns at the national level

2020 Achievements

Produced over 40 awareness posters, launched over eleven (11) awareness campaigns, three (3) specialized guideline documents

Increased social networks presence by four (4) folds

Reached over one (1) million visitor to cert.gov.sa

Activities & Operations

Achievement

Produced over 40 awareness posters, launched over eleven (11) awareness campaigns, three (3) specialized guideline documents

Increased social networks presence by four (4) folds

Reached over one (1) million visitor to cert.gov.sa

2021 Planned Activities

Launch the national cybersecurity awareness campaign

Launch the national cybersecurity LMS

Organize regional CERT conference

"Increased social networks presence by four (4) folds"

SOMALIA

Somalia Computer Emergency Response Team / Coordination Centre

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

Background

Somalia Computer Emergency Response Team / Coordination Centre (SomCERT/CC) is the first national CERT in Somalia. SomCERT/CC provides cybersecurity incident handling, promoting cybersecurity awareness, as well as coordinating cybersecurity issues. SomCERT/CC collaborates with government agencies, organizations, telecom operators, national critical infrastructure operators, academia, ISPs, and other relevant entities to handle cybersecurity incidents in Somalia and various cybersecurity initiatives worldwide. SomCERT/CC provides timely warning, support, and advisories to all its constituents in preventing and handling cybersecurity incidents.

Establishment

SomCERT/CC was established in 2019, by the National Communications Authority (**NCA**), as a section under the Cyber Security Department with the objective of securing Somalia's cyberspace and providing an official point of contact to handle cybersecurity incidents for the Internet community.

Resources

Incident Handling and Response Team

Cybersecurity training and awareness team

Information Sharing team

International Coordination team

Constituency

Ministries and Government Agencies

Law Enforcement Agencies

Regulatory Bodies

National Defence

Banks and Finance

ICT, ISP, and Telecommunication Providers

Academia

National Critical Infrastructure Operators

Highlights of 2020

Summary of Major Activities

Serve as a trusted point of contact at the national level

Provide cybersecurity incident handling

Develop policies, procedures, and guidelines

Provide advices to the constituencies

Manage and release cybersecurity alerts

Cooperate with the local and international CERTs

Provide cybersecurity training and awareness

Achievements

Conducted a national cybersecurity assessment with the Cybersecurity Capacity Centre for Southern Africa and Global Cyber Security Capacity Centre (**GCSCC**)

SomCERT provided cybersecurity awareness training to NCA of Somalia and the Ministry of Communications and Technology (**MoCT**), Federal Government of Somalia

Developed and designed the official SomCERT logo and website - *www.somcert.gov.so*

Provide cybersecurity awareness workshop to ICT and Telecom students from the local universities

Activities and Operation

Events organized by the organization / agency

Conducted the cybersecurity assessment with Cybersecurity Capacity Centre for Southern Africa and GCSCC using the Cybersecurity Capacity Maturity Model for Nations (**CMM**) at the national level

Conducted cybersecurity awareness workshop to NCA staffs

Published the general cybersecurity awareness video (Somali Version) entitled "*Stay safe and secure. while working from Home*" on the Social Media *https://twitter.com/SomaliaNCA/status/1259544979967561734?s=20*

Facilitated and sponsored Somali Network Operators Group (**SomNOG**) workshop

Events involvement

Somcert and NCA hosted the annual celebration of Girls in ICT day on April 2020 to empower and encourage girls and young women to embrace careers in the growing

field of ICT in collaboration with the MoCT Somalia

Partcipated in GFCE

Participated in the 8th Arab Regional and OIC-CERT Cyber Drill 2020

Participated in the "*National Cybersecurity Policy: Balancing Risk and Innovation*" webinar provided by United States Telecommunication Training Institute (**USTTI**)

Participated in the training on Cybersecurity Policy and National Strategy and Policy for Cybersecurity and Incident Response, by Software Engineering Institute, Carnegie Mellon University, USA and the CERT of Mauritius

Participated in the OIC-CERT 12th Annual Conference 2020 (virtual) - 23 & 24 Nov 2020 and CyberSecurity Malaysia's Webinar - *25 Nov 2020*

Participted in the Arab Information & Communication Technology Organization (**AICTO**) - KISA Forum - South Korean Cybersecurity Policies and incidents Handling Experience, New Trends - *10 Nov 2020*

Participted in the online training "*Mobile Security*", host by aeCERT - *21 Sep 2020*

Participated in the online training "*Managing Security Incident Response During Covid Outbreak: A Lesson Learned*" hosted by BSSN Indonesia - *3 Sept 2020*

2021 Planned Activities

Develop the National Cybersecurity Strategy and Policy

Develop the Cybersecurity and Cybercrime Legislation

Develop the National Guidelines for the Protection of National CII

ISO 27000-series or similar Cybersecurity certification for SomCERT

Assessment for establishing a cyber forensics laboratory for law enforcement,

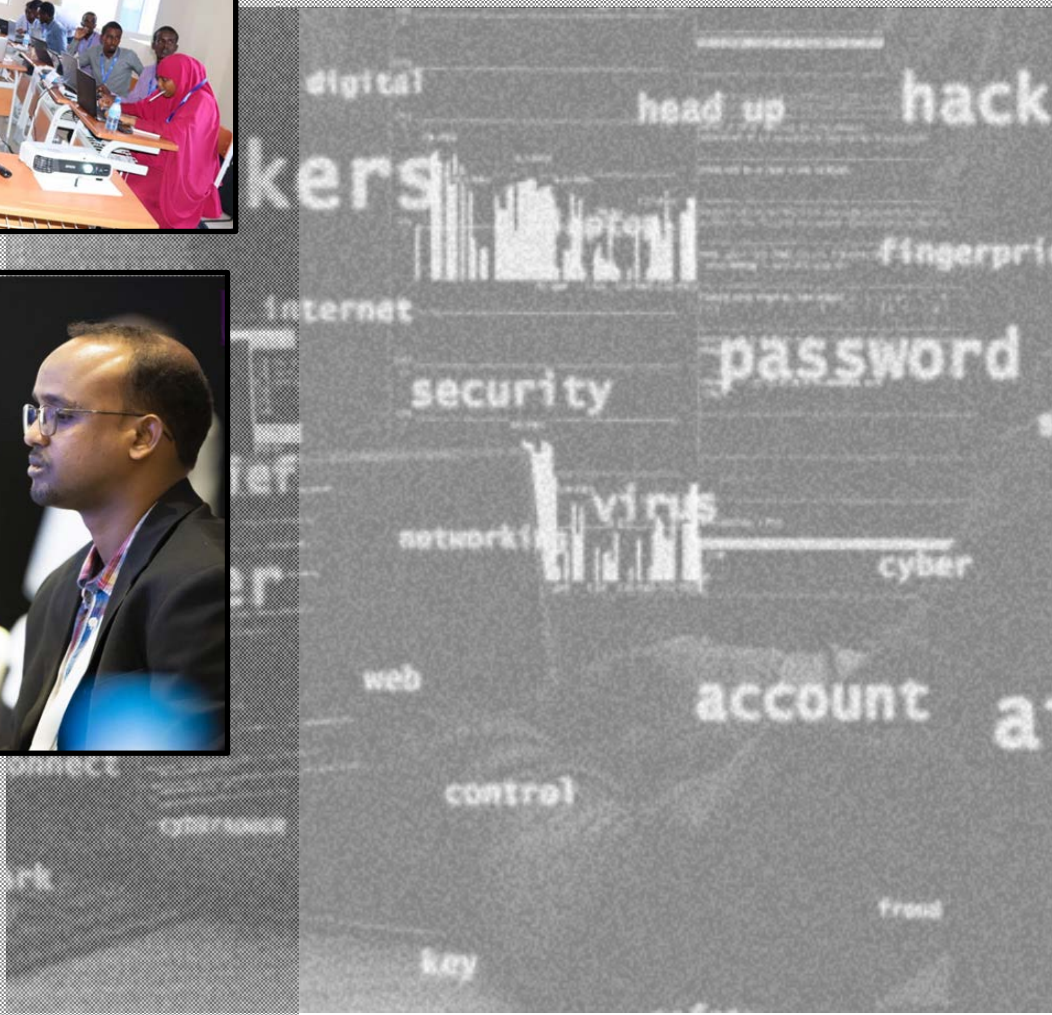
with estimates and technical specifications

Capacity Building for government officials at technical / working levels, law enforcement and judiciary

Program with local universities to provide practical cybersecurity training to students and produce new generations of cybersecurity analysts in Somalia

Cybersecurity Innovation Center


Workshop for empowering girls through ICTs


digital
head up
hack
kers
internet
password
security
virus
cyber
web
account
control
fraud
key

TUNISIA

National Agency for Computer Security

National Agency for Computer Security (TunCERT)

Background

National Agency for Computer Security (**NACS**) TunCERT carries out general supervision over computer systems and networks appropriate to the diversified public and private organization.

Establishment

Law N°5 of 3 Feb 2004 relating to computer security and to the organization in the field of computer security and laying down the general rules for the protection of computer systems and networks.

Resources

78

Constituency

National: private and public

2020 Highlights

Summary of Major Activities

The co-organization of a seminar on 5G technology under the theme "*5G Development in Cybersecurity and Readiness*"

The co-organization of a symposium via the web under the slogan "*Developing the Fifth Generation Network in the Field of Cybersecurity and Readiness*" in cooperation with the Institute for Security Studies and Future Strategies (**IPASSS / IPA3S**), and Huawei

The announcement for the publication of samples of reference elements in the field of computer security

The announcement of the provision, for the benefit of Tunisian organizations, of TdRs to create a system

The announcement of the publication of samples of reference elements in the field of computer security

Participation of TunCERT in the 1st Global Cyber Drill exercise during the period from 27 Oct – 5 Nov 2020 organized by the ITU ARCC for Cybersecurity. ITU ARCC has a participation of more than 400 experts from 57 countries. The exercise focused mainly on the cyber threats and challenges resulting from the Covid 19 pandemic in the healthcare sector

A partnership between Tunisian Internet Agency and the National Agency for computer security in the field of protecting the national cyber-space

2020 Achievements

As part of the National Strategy for Cyber Security, the NACS and the Centre for Studies and Research Telecommunications signed two cooperation agreements

Assisting the Financial CERT to have the recognition of FIRST

Activities & Operations

Events organized by the organization / agency

Safer Internet Day

CyberSec & Blockchain

NCSC 2nd Edition

Tunisie Telecom Security Day 3rd Edition

Events involvement

National Cyber Security Strategy Action Plan

OIC-CERT 12th Annual Conference 2020

Technical Assistance and Information Exchange (**TAIEX**) Multi-Country Workshop

ITU 2020 Global Cyber Drill

Symposium for Africa and Arab Regions

OIC CERT Drill 2020

aeCERT 2020

Achievements

Awareness campaigns to talk about recommendations concerning the effects of covid 19 : "*The New Wave of Phishing on Social Networks*"

A guide for best practices to protect personal identity and distance work

Video conference in collaboration with national CERTs in accordance with the health provisions imposed to fight against spread of covid 19

2021 Planned Activities

The activities of 2021 are still on going


الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
Guide pour la protection de l'identité numérique
tunCERT


LES TYPES DES INCIDENTS TRAITÉS
PHISHING
EXTORSION
RANSOMWARE
TYPOSQUATTAGE

TURKEY

National Cyber Security Incident Response Team

National Cyber Security Incident Response Team (TR-CERT)

Background

National Computer Emergency Response Centre (**USOM, TR-CERT**) was established by the Information and Communication Technologies Authority (**ICTA**) to determine threats against national cybersecurity, take measures for reducing or elimination of the impact of a likely cyber-attacks and to share information with the defined actors.

The mission of TR-CERT is to protect the Turkish government's cyberspace, along with critical infrastructures, both public and private, such as the energy production and distribution, water management, and telecommunication institutions and facilities in Turkey.

Establishment

TR-CERT was established on the 27 May 2013 by ICTA in accordance with the 4th. clause "*National Cybersecurity Strategy and 2013-2014 Action Plan*" (Turkish Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı) issued by the Cabinet of Turkey and published in the Official Gazette of the Republic of Turkey.

Resources

TR-CERT benefits from the resources of ICTA which is the national regulatory authority of Turkish electronic communication sector and has a special governmental budget for national cybersecurity activities.

Constituency

TR-CERT is the national CERT of Turkey and its constituency covers the whole country including the public and private sectors and individuals.

2020 Highlights

Summary of Major Activities

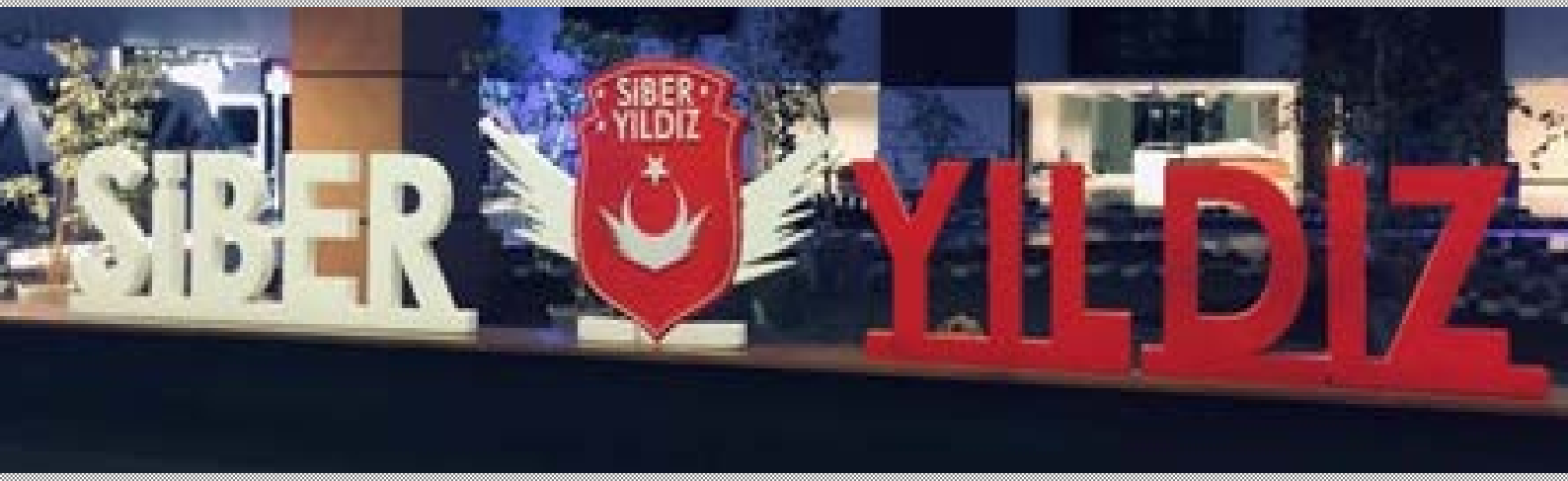
The Cyber Star (Turkish: Siber Yıldız), a 24-hour online capture-the-flag cybersecurity competition organized by TR-CERT for the third time, had over 20,000 contestants. - *25 Dec 2020*

TR-CERT's SOC was officially opened - *10 Feb 2020*

Cooperating with "ICTA Academy" (Turkish: BTK Akademi), TR-CERT has given various cybersecurity trainings, ranging from web application security to computer forensics. In this context, approximately 5,000 participants were trained

With the publication of the National Cyber Security Strategy and Action plan of 2020-2023, TR-CERT starts to improve its capabilities in the fields of cyber threat intelligence, training of the cybersecurity personnel, determining the maturity levels of the existing personnel

AVCI, AZAD and KASIRGA projects, which are developed with completely institutional resources, make significant contributions to the national cybersecurity. With AVCI application, malware-infected systems and command control centres are being identified, and studies are carried out to determine the slave computers that have been included in botnets by means of machine learning and artificial intelligence through AZAD application. On the other hand, starting with the weaknesses of critical public institutions and critical infrastructures and including the Internet open resources of the country, the monitoring activities to ensure continuity of service and vulnerability search are conducted through the KASIRGA project.



2020 Achievements

43.121 malicious links (URL, IP, domain) used in malware and for phishing has been identified, controlled, and blocked to access at infrastructure level.

12.533 cybersecurity notifications have been made to the institutions / organizations / enterprises

5003 cybersecurity experts from 1804 Computer Emergency Response Teams registered to TR-CERT, are coordinated through the CERT Communication Platform established within the organization of TR-CERT

The third Cyber Star Competition was held with 2895 participants - *25 Dec 2020*

With the aim of training the human resources needed by the country in the field of cyber

security, the capabilities of cybersecurity experts operating in critical sectors are developed by increasing the capabilities of cybersecurity experts operating in critical sectors through cybersecurity trainings that are integrated with ICTA Academy. In addition, trainings for high school and university students and new graduates are also available to the public and online trainings for CERTs are organized. In this context, approximately 5,000 participants were trained

Cooperation activities continue with countries and international organizations in the field of cyber security. TR-CERT is a member of organizations such as FIRST, Trusted Introducer (**TI**), Cybersecurity Alliance for Mutual Progress (**CAMP**), North Atlantic Treaty Organization (**NATO**) Malware Information Sharing Platform (NATO-MISP). Recently, membership procedures to the OIC-CERT have been completed. Threat intelligence sharing activities with these organizations are continuing. In addition, on behalf of the country, TR-CERT and ICTA contribute to the activities of organizations such as the United Nation (**UN**), ITU, NATO, OSCE, Group of Twenty (**G20**) and Organisation for Economic Co-operation and Development (**OECD**) in the field of cybersecurity.

Activities & Operations

Events organized by the organization / agency

The third Cyber Star Competition was held on 25 Dec 2020. Cyber Star consist of the series of “capture the flag” type of competitions that are organized by TR-CERT within ICTA. The objective of the project is to reach the citizens who are talented and interested in cybersecurity and provide them with the opportunity to improve themselves. This also include improving the awareness in cybersecurity. Additionally, Cyber Star contributes towards TR-CERT's efforts in capacity building.

Events involvement

TR-CERT continues to participate and contribute to various international cybersecurity exercises such as NATO Locked Shields, NATO Cyber Coalition, and NATO Crisis Management Exercise. Some of the other events attended are TR-CERT - CSIRT Advisory Meetings, Energy Sector CSIRTs Meeting.

Achievement

During the pandemic period, with the local and national systems called AVCI, AZAD and KASIRGA using artificial intelligence technologies, have detected 750 fake conference applications and 25,380 weaknesses in remote management services. With the Sinkhole application, institutions and organizations accessing malicious links blocked by TR-CERT are detected and informed

119 malware examinations and 569 malware information related to COVID-19 were shared with CERTs. 1657 harmful droppers and command control centres related to COVID-19 have been blocked

With the ATMACA project, which works in integration with KASIRGA and developed with internal human resources, the risks of more than 436 vulnerabilities have been proactively prevented by regular checks for each of the 16 million IP addresses in total. Domestic and national KULE software has been developed to manage data more efficiently by expert analysts and to deliver the information on the detected cybersecurity deficiencies to the relevant parties faster

Cyber Star contributes, improving the awareness in cybersecurity and TR-CERT's efforts for capacity building

2021 Planned Activities

The National Cyber Security Exercise will be organized

CERT maturity model will be developed and implemented at national scale

Cyber Star competitions and cybersecurity training activities w ill be on going on.

AVCI, AZAD and KASIRGA using artificial intelligence technologies, have detected 750 fake conference applications and 25,380 weaknesses in remote management services

UNITED ARAB EMIRATES

UAE Computer Emergency Response Team

UAE Computer Emergency Response Team (aeCERT)

Background

https://www.tra.gov.ae/aecert/en/home.aspx

National Computer Emergency Response Team - **aeCERT**) launched a number of initiatives aiming to raise cybersecurity awareness and activate all initiatives that would spread awareness among the different groups of society towards the importance of cybersecurity. aeCERT has been established to improve information security standards and practices, protect and support UAE ICT infrastructure from online risks and breaches, and build a secure and protected ICT culture. aeCERT goals include enhancing the cybersecurity law and assisting in the creation of new laws, enhancing information security awareness across the UAE, and building national expertise in information security, incident management, and computer forensics. The Section also provides consultation services to government entities regarding IT management and standards.

aeCERT international participation:

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

Establishment

aeCERT was established by the Decree 5/89 of 2008 issued by the Ministerial Council for Services.

Resources

aeCERT services:

- ***Computer emergency response services***

Responding to computer emergencies in federal organizations

Providing cyber forensic services through aeCERT's Evidence Lab

Infrastructure monitoring services

- SIEM infrastructure monitoring solution
- Website defacement monitoring services

Providing technical tip documents

Anti-phishing email services

Information quality assurance services

Vulnerability assessment services

Penetration testing services

Cybersecurity awareness, guidelines, and training services

Federal entity awareness

Public awareness

Awareness through the media

Constituency

Governmental and semi-governmental entities

Some of the private entities (especially banks)

The public

Academic institutions

2020 Highlights

Summary of Major Activities

Computer emergency response services

944,209 cyber incidents addressed

2,085 cyber incidents has been dealt with

2,972 sites were tested against defacement

During COVID-19

Developed a guideline about how to secure a VPN

Used mobile forensics testing lab

Used Aramex to transfer hard disk drives

Established 16 specialized training courses

Designed a training plan for each employee based on the NICE framework from NIST

Cybersecurity awareness services

213 awareness sessions provided.

15,070 people attended awareness sessions

3 awareness sessions conducted via TRA Virtual Academy and total number of beneficiaries is 13,085

4 specialized training conducted for 477 beneficiaries

During COVID-19

Provided remote lectures and created an awareness package for entities about remote working security

Raised awareness among the students and parents by using awareness videos using train the trainers methodology

Provided 3 counselling sessions for 2,115 parents - outside working hours.

Support and sponsorship of the HAVOC Virtual Specialist Conference

Information quality services

13 vulnerability reports prepared

306 vulnerability assessment testing

340 penetration testing services

Attending 7 training courses within the training plan

During COVID-19

Conducted a vulnerability testing for the authorization system in Dubai '*movePermit*'

Conducted 4 urgent off-plan checks

Developed and fully implement a FedNET Vulnerability Management Plan

Compliance services

456 Compliance Requests Completed

133 applications were completed outside of working hours

5 requests were completed in the Eid vacation

The team receives requests from the organization and from the Federal Network all the time

Attending 11 training courses within the training plan

Infrastructure services

New Domain Controller installation transferring all aeCERT servers to a new vCenter

Install Proofpoint Email Gateway (mail protection, mail firewall, spam detection, virus detection)

Network clean-up, including Switches - Routers – Firewalls

aeCERT to FEDnet MPLS Connectivity– Phase 1

Network Upgrade for aeCERT - Phase 1

Monitoring Team Preparation (Hardware / Software)

During COVID-19

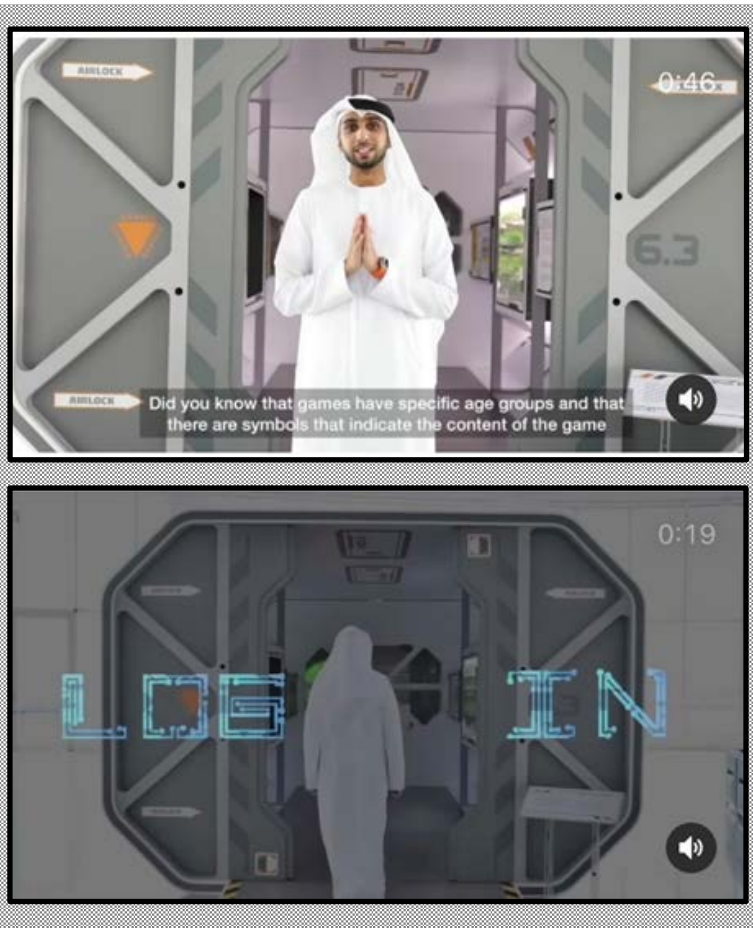
Developed A guide for securing VPNs, JumpServers and MFAs

Network Management System (**NMS**) installation

Password management system installed

Adjust Jira system settings for the infrastructure team

Attending 7 training courses within the training plan



2020 Achievements

aeCERT launches the National Cybersecurity Capacity Building Program. A core program within the National Cybersecurity Strategy. The Program aims to develop highly efficient national capabilities in protecting the cyberspace and addressing relevant risks. The Program also aims to develop the capabilities of youth in cybersecurity, whether professionals or those working in areas related to IT and Computing, or students and amateurs, thus contributing to enhancing the readiness of UAE to respond to cyber incidents and supporting research and innovation, while safeguarding the digital infrastructure of the country.

aeCERT launches Sannif initiative. It is a main supporter of the National Program for Digital Wellbeing, which seeks to raise awareness about digital risks and challenges and promote safe and positive use of digital technologies and Internet. The program seeks to support individuals of all ages. An initiative that aims to classify and display the risks of video games available on various gaming platforms. Sannif allows searching for any video game and display its details, risks, and appropriate age, in addition to the platforms it supports. The platform also provides a list of family games as well as explanation of the potential risks in games. Sannif aims to be a reliable source for evaluating video games. It helps parents select the appropriate games for their children by providing the necessary data, to protect children from the risks of such games.

Established a mobile forensic examination lab:

- Smart application launched to publish security advisories
- Endpoint Protection service launched
- Source code security review service launched
- Develop and improve security systems for the Federal Network
- Developed an integrated guide for cybersecurity jobs
- Developed an interactive training material for children

Activities & Operation

Events organized by the organization / agency

CyberPro: an initiative to build the capacity of employees working in cybersecurity and IT-related fields through free monthly training courses focused on specialized cybersecurity topics of various levels presented by experts in the field. Each course spans one to two days and features theoretical explanations and enhanced practical exercises.

Objectives:

- Fostering expertise of cybersecurity professionals by providing in-depth courses in the field
- Educating IT workers and fresh graduates on cybersecurity principles and core themes
- Increasing the readiness of cybersecurity professionals to respond to cyber-attacks and resulting incidents

Beneficiaries:

- Cybersecurity specialists
- Specialists in Information Technology, Computer Engineering, and Computer Science
- University students and cybersecurity enthusiasts

Events Involvement

Safer Internet day: aims to raise awareness of emerging online issues and current concerns

Participate in '*The National Bullying Prevention Week'*. Raising awareness among the students & parents about the prevention of cyber bullying

Cybersecurity ambassadors 'Phase 2'

- This initiative aims to train a number of young students so that the trainee acts as the cybersecurity ambassador and familiarizes their colleagues with cybersecurity principles
- Increase awareness at schools
- Equipping ambassadors with some cybersecurity-related techniques and skills
- Identify and assess cybersecurity competencies

Achievements

Chairing the meeting of the National CERTs Committee in the GCC countries

Participation in the Arab League meetings related to cybersecurity

Chair the meeting of the Child Online Protection Team at the International Telecommunication Union

Provided 6 training workshops for information security professionals in the OIC countries

Established an indicative framework for security awareness in the OIC countries

2021 Planned Activities

Celebrating Safer Internet Day

Cybersecurity Hackathon

National Cyber Drills

UZBEKISTAN

Uzbekistan Computer Emergency Response Team

Uzbekistan Computer Emergency Response Team (UZCERT)

Background

Uzbekistan Computer Emergency Response Team - UZCERT service, operating as a unit under the State Unitary Enterprise 'Cybersecurity Center'. This unit is focused on national cooperation and interaction with the operators and providers, as well as the users of the Internet, in providing the necessary support when responding to cybersecurity incidents. The UZCERT service carries out the necessary analysis of incident artefacts, establishes the causes and consequences of the incident, and prepares recommendations for effective counteraction to virus and hacker attacks. This approach has resulted in a positive trend in information and cybersecurity threats and incidents, including through continuous training of the employees in the field of computer forensics, malware analysis, and the world's best practices for responding to cybersecurity threats and incidents.

Given the cross-border nature of cybersecurity threats and incidents, the service aims to collaborate widely with foreign partners to maximize the opportunities and experience of the world community in the fight against cyber-threats and cyber-crimes.

The result of this approach is the positive dynamics of threats and incidents of information and cybersecurity, which is also due to the continuous training of the employees in the field of computer forensics, malware analysis, and the best world practices in responding to threats and incidents of cybersecurity.

Establishment

The increased attention on the issues of cybersecurity is backed by the Presidential Decree of '*On the State Program for the implementation of the National Action Strategy on Five Priority Development Areas*' signed in 2017. Among other, the decree will ensure further improvement of cybersecurity

in the country, which is one of the most important priorities. The tasks of implementing government initiatives in the field of information and cybersecurity were assigned to the '*Information Security Centre*' created in 2013, and years later, following the government decision in 2019, was transformed into the State Unitary Enterprise (**SUE**) of 'Cybersecurity Centre' along with an increase in its roles as the body with executive responsibility on state policy in the field of information and cybersecurity.

Resources

Government

Constituency

UZCERT is responsible for providing and supporting information and cybersecurity for all users and resources operating in the national Internet segment (UzNET) of the Republic of Uzbekistan.

2020 Highlights

Summary of Major Activities

Indeed, 2020 was remarkably a challenging year for UZCERT as well as its partners. However, the team at UZCERT stayed positive and tried to confront the challenges presented by the pandemic. The team participated in several online conferences, established several joint agreements with new international friends, achieved memorandum of understandings, and most importantly, contributed to make the UZNET a safe place.

UZCERT is grateful to the partners for being phenomenally flexible during the hard times and helping the team to make 2020 a valuable year.

2020 Achievements

Participation in the 22nd annual teleconference of the Operations Committee of CAMP Republic of Korea

By the initiative of the Cybersecurity and Infrastructure Security Agency (**CISA**) of the U.S. Department of Homeland Security, UZCERT took part in the 3rd Annual National Cybersecurity Summit - CyberSummit 2020

Participation in the 32nd FIRST Annual Conference

Participation in the 12th Annual OIC-CERT Conference

Activities & Operation

Events organized by the organization / agency

The SUE 'Cybersecurity Centre' regularly conducts various seminars and training courses on various issues of information security and cybersecurity for authorized employees of state bodies and institutions of the Republic of Uzbekistan.

Events Involvement

In 2020, specialists of the SUE "Cybersecurity Centre" attended various courses in the field of information and cybersecurity, such as:

The initiative of the CAMP Secretariat (Republic of Korea), participation in the 20th Teleconference of the Operations Committee of the Alliance for Cybersecurity in Mutual Progress

Took part in the initiative of the OIC-CERT online training provided by aeCERT and BSSN with the following topics:

- Security of remote work (Remote Working Security)
- Social Engineering
- Malware

- Management of the technical journal of the 4th industrial revolution
- Managing security incident response during COVID outbreak: a lesson learned
- Mobile Security
- Computer security
- Data Breach Response: Challenges and Strategies (co-hosted by Indonesia's National Cyber Crypto Agency (**BSSN**))
- Safety in social networks
- Email Security

Participation in an online conference on the topic '*Cybersecurity of the Republic of Uzbekistan: Strategic Session'*, organized by Kaspersky Lab (Russian Federation)

Participation in the online interactive exercises '*Cyber-Polygon 2020*'

Participation in the online training on '*Management of the technical journal of the 4th industrial revolution*' organized by OIC-CERT

Participation in an online master class organized by the Tashkent Inha University and together with the Russian company GROUP-IB on the topics '*Modern cybersecurity and methods of struggle*' and '*Fundamentals of computer forensics*'

Participation in an online conference with Kaspersky Lab on the topic '*Cybersecurity in Uzbekistan*'

Participation in the cyber exercises 8th Arab Regional & OIC-CERT Cyber Security Drill 2020

Participation in the online training on '*Managing security incident response during COVID outbreak: a lesson learned*' organized by OIC-CERT

Participation in the 14th International Cyber Security Conference organized by Cisco India

Participated in the cyber-training CyberDrill organized by the OIC-CERT

Participated in an online business meeting organized by the CAMP in the format of video conference

Participated in the Prague virtual conference on security in 5G networks, organized by the National Agency for Cyber and Information Security (**NCISA**) of the Czech Republic

Participated in a business meeting organized by CAMP in the format of a videoconference with Monitor app

Participation in an online videoconference organized by the OSCE on the topic: '*Central Asia Regional Online Training FROM CYBER CRIME TO TERRORISM: Effective Online Investigations and the Role of Digital Forensics'*

Participate in the online training organized by OIC-CERT and conducted by BSSN with the title '*Responding to data breaches: problems and strategies'*

Participate in the online conference on '*Cybersecurity Advocacy for a Safer Cyber Environment*', an initiative of the CAMP

Participation in an online video conference organized by CNCERT/CC on the topic '*Cooperation in an emergency in the field of cybersecurity and response in time to Covid-19*'

Achievement

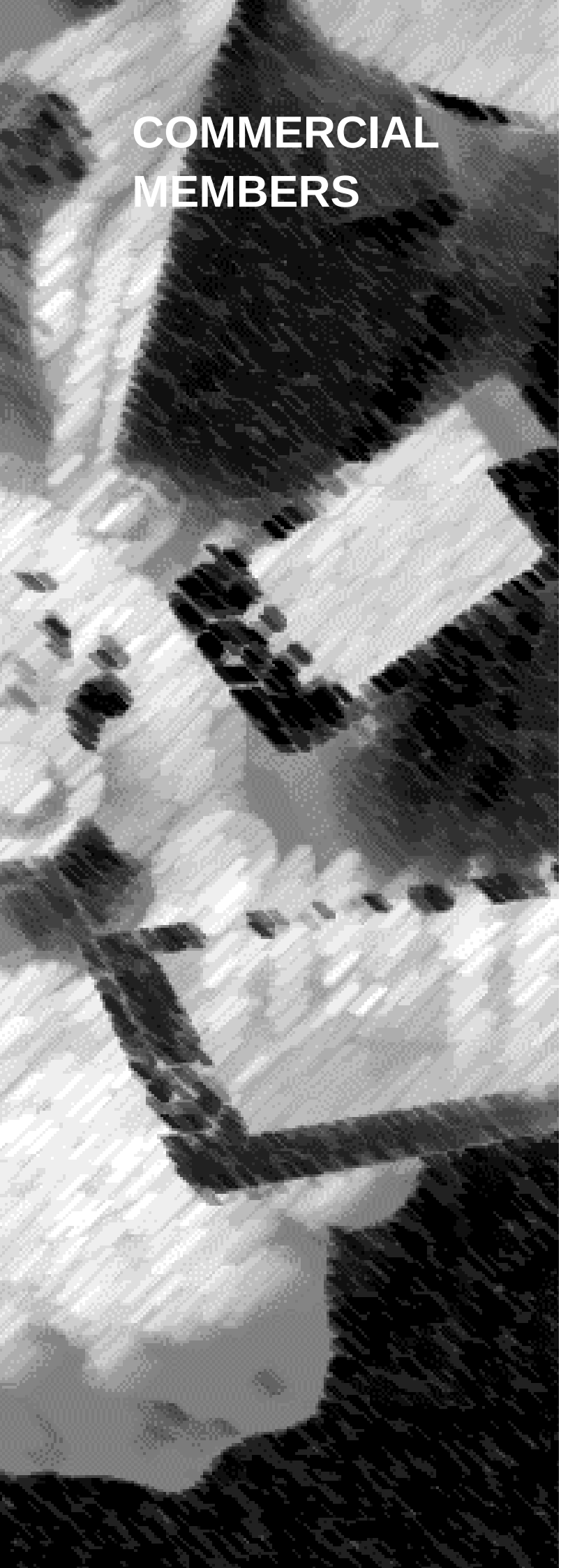
Signing a Memorandum of Understanding with the aeCERT and CERT India (CERT-In)

2021 Planned Activities

Nowadays, SUE 'Cybersecurity Centre' is actively working on the coordination and signing of MoU with foreign departments and organizations CERT. In 2020, UZCERT has achieved agreements for joint activities with following countries such as the Republic of Kazakhstan, Republic of Poland, Russian Federation, the United Arab Emirates, Japan and China, as well as with private antivirus

software companies such as KasperskyLabKz and Dr.Web. The main goal for the 2021 is continuous development in the field, and active cooperation with foreign partners and signing of MoU with new partners. In addition there is a collaboration with the ITU and the Japanese Computer Emergency Response Team (**JPCERT/CC**) who is actively supporting UZCERT team to achieve full FIRST membership status.

"...grateful to the partners for being phenomenally flexible during the hard times and helping the team to make 2020 a valuable year"



COMMERCIAL MEMBERS

Group-IB

(Computer Security Incident Response Team GroupIB)

Background

CERT-GIB is the Computer Emergency Response Team created by global cybersecurity company Group-IB. It was launched with the mission to immediately contain cyber threats, regardless of when and where they take place and who is involved.

CERT-GIB combines the power of human intelligence with technological prowess to offer the most effective response and remediation actions.

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

Establishment

10 Mar 2011

Resources

Human intelligence

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

CERT-GIB works closely with Group-IB's Digital Forensics Laboratory, Threat Intelligence & Attribution, and Investigation Teams.

Proprietary technology

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

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

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

Combined, Group-IB technological capabilities include:

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

Unmatched expertise

CERT-GIB has spent over 65,000 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, the Tactics, Techniques and Procedures (**TTP**s), and movements.

International cooperation

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

CERT-GIB also actively collaborates with top level Russian domains to block dangerous websites.

Constituency

Service Provider Customer Base

CERT-GIB's constituency includes organizations from Media, Law Enforcement Agencies

Government Sector, Internet Service Providers,

Private Sector and Critical Infrastructures

2020 Highlights

Summary of Major Activities

65000+ hours of Digital Forensics and Incident Response

3 products launched: 1-Threat Intelligence and Attribution; 2-Threat Hunting Framework product; 3-Fraud Hunting Platform product

Managed Security Service Provider (**MSSP**) & Managed Detection and Response (**MDR**) partner program launch

Security related information dissemination

International cooperation with other CERT/CSIRT teams

Cybersecurity awareness events (20 webinars; 16 events) in 2020

2020 Achievements

Product Launch

Threat Intelligence and Attribution product launch

Threat Hunting Framework product launch

Fraud Hunting Platform product launch

Program Launch

MSSP and MDR Partner Program (*https://www.group-ib.com/mssp-mdr-partner. html*)

Analytical and Technical Reports

Hi-tech crime trends 2020 / 2021 (*https://www.group-ib.com/resources/threat-research/2020-report.html*)

UltraRank: '*The unexpected twist of a JS-sniffer triple threat*' (*https://www.group-ib.com/resources/threat-research/ultrarank.html*)

RedCurl: '*The Pentest You Didn't Know About*' (*https://www.group-ib.com/resources/threat-research/red-curl.html*)

Online Piracy Research: '*Jolly Roger's Patrons*' (*https://www.group-ib.com/resources/threat-research/black-jack.html*)

Fxmsp: '*The invisible god of networks*' (*https://www.group-ib.com/resources/threat-research/fxmsp-report.html*)

Ransomware White Papers:

'Egregor ransomware: The legacy of Maze lives on' (*https://www.group-ib.com/whitepapers/egregor-ransomware.html*)

'*Lock like a Pro: How Qakbot fuels enterprise ransomware campaigns*' (*https://www.group-ib.com/whitepapers/prolock.html*)

'Ransomware Uncovered: Attackers' Latest Methods' (*https://www.group-ib.com/whitepapers/ransomware-uncovered.html*)

New offices

Opened European HQ in the Netherlands, Amsterdam

Opened representative offices in Vietnam and Malaysia

Presence in Spain, Italy, South Africa, UAE, South Korea, Australia, Pakistan

Established CERT branch in Innopolis (*http://madeintatarstan.com/en/node/502*)

Annual conference

CyberCrimeCon'20 (*https://virtual.group-ib.com*)

Publications

7491 publications - Bloomberg, the Guardian, The Economic Times, Bleeping Computer, Business Insider, ZDNet, Fox News, etc.

50 press-releases

13 technical blogs

Membership

Became a member of the Merchant Risk Council

Became a member of the Anti-Phishing Work Group

Signed a partnership with FS-ISAC

Special operations

Carding Action 2020: Group-IB supported Europol-backed operation (*https://www.group-ib.com/media/carding-action-2020/*)

Operation Falcon: Group-IB helps INTERPOL identify Nigerian BEC ring members (*https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group*)

Activities & Operation

Events organized by the organization / agency

Group-IB lecture in Kazan Federal University

Training for MSSP partners from Saudi Arabia

Cyber Drill for MSSP partners from Saudi Arabia

Education for MSSP partners from Italy

CyberCrimeCon 2020 Global

Several online events with coordination centre for TLD Russia

Fraud Day in Albania, Bulgaria, Slovenia, Croatia, Serbia

Threat day ‘Hunt or be Hunted’

Threat Day with Sanfinity

Threat Day with NDS

Threat Intelligence Sharing Session

Webinars

- Digital risks 2021: Scam trends and projections
- Preventable Disaster: Hunting for Egregor Operators in Your Network
- Europe hit by ransomware: real-life cases and insights into active groups
- Outwit ProLock: The ins and outs of Qakbot's enterprise ransomware campaigns
- Zen or Skill to Catch the Hacker
- RedCurl: New corporate espionage group exposed
- Leaving sandboxes behind: the rise of Malware Detonation Platforms
- Joker’s Stash– The Biggest Dump on the underground market
- Scenario-Based Pentesting and Security Monitoring
- Retail Business vs. Online Scammers: The Battle Against Illegal Brand Exploitation
- Fxmsp: The story of 1 hacker who sold access to networks
- Stay one step ahead: TTPs used by ransomware groups in 2019
- A Playbook of 'Perswaysion' Phishing Campaign
- Investigation beyond borders
- How Fraudsters Attack Their Victims in Early 2020: Case Studies
- If I have a SOC, do I need Compromise Assessment?
- Intelligence-driven threat hunting, or don't let the hunter become the prey
- 6 Symptoms of Disease: Risks for Online Pharmaceutical Market
- Open API security: Clarity instead of obscurity
- The 3 types of online fraud attack you're most likely to face in 2020

Events involvement

"*CTF Cybershock*" by CERT.LV

OIC-CERT Annual Conference 2020

The 62nd TF-CSIRT meeting - Virtual TF-CSIRT

FIRST Virtual Symposium for Latin America and Caribbean Regions

OAS Cybersecurity Virtual Symposium Incident Response track

FS-ISAC Member meeting

OT-ISAC Virtual Summit

FS-ISAC Training Days

CyberAttack KL Conference

CyberAttack Singapore Conference

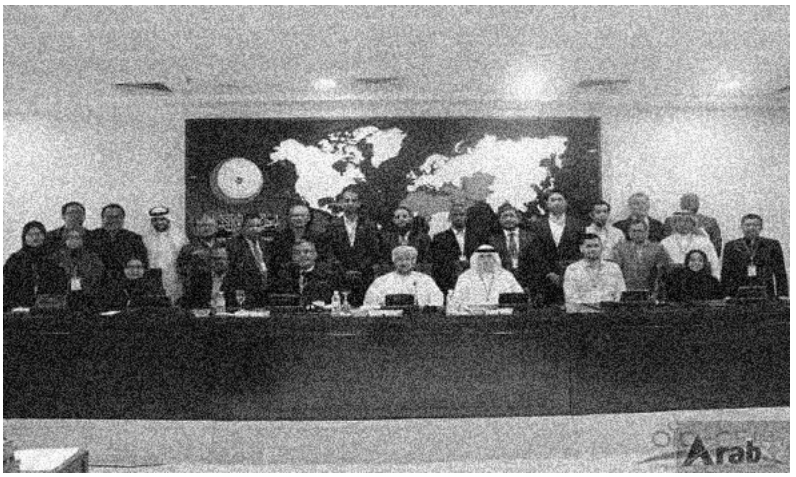
VT Cybersecurity summit

FS-ISAC APAC

GovWare Conference

Mena Cybersecurity Summit

RISK 2020 Conference



Huawei

Background

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

Huawei booth at GITEX Technology Week 2020 held in Dubai, United Arab Emirates

The vision and mission are to bring digital to every person, home, and organization for a fully connected, intelligent world. To this end, Huawei will drive ubiquitous connectivity and promote equal access to networks; bring cloud and artificial intelligence to all four corners of the earth to provide superior computing power where needed, when is needed; building digital platforms that is more agile, efficient, and dynamic; redefine user experience with artificial intelligence (**AI**), making it more personalized for people in all aspects of life. Huawei has operated in the Middle East region for over 20 years now, with Bahrain as the regional headquarters and the UAE as the MEA business centre, with Dubai being one of the six global cybersecurity centres. Huawei has identified and prioritized cybersecurity since 2005 when the Huawei Product Security Incident Response Team (**PSIRT**) is formed. PSIRT manages the receipt, investigation, internal coordination, and disclosure of security vulnerability information related to Huawei offerings and it is an important window to disclose the vulnerability of Huawei products. Huawei PSIRT became a FIRST member in 2010 and adheres to ISO/IEC 29147:2018. Subsequently Huawei published the first cybersecurity white paper in 2012, the second one in 2013, the third white paper in 2014, and a fourth in 2016 and most recent position paper in 2019.

Establishment

1987

Resources

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

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

Constituency

Huawei's customers in the global ICT eco-system that Huawei is a part of, covers over 170 countries and regions where Huawei provide products, services, and end-to-end solutions to carrier network clients, enterprise customers, government, and end-user consumers.

2020 Highlights

Summary of Major Activities

Following is a summary of key activities that Huawei has been delivering in past years as part of its key strategy that prioritise security over business and supporting our

TECH4ALL long-term digital inclusion initiative that is aligned with United Nations' Sustainable Development Goals:

Continue to invest and participate in open and transparent platforms globally on apolitical and technical insights sharing pertaining to cybersecurity. For instance, despite the Covid-19 pandemic, Huawei Cybersecurity Transparency Centres (**HCSTC**) such as the one in Brussels continue to operate and host guests virtually from all over the world and provides a platform for guests to experience cybersecurity with Huawei's products and solutions, in areas including 5G, IoT, Cloud, etc. and showcase Huawei's end-to-end (**E2E**) cybersecurity practices, from strategies and supply chain to R&D, products and solutions, providing clarity in Huawei's E2E security approach covering 12 areas: (1) Strategy and Governance, (2) Laws and Regulations, (3) Processes, (4) Research & Development, (5) Supplier Management, (6) Manufacturing and Logistics, (7) Security Service Delivery, (8) Validation and Certification, (9) Traceability, (10) Defect and Vulnerability Resolution, (11) Human Resources, and (12) Audit. The HCSTC provides the platform for collaboration with the industry and standard organizations, to promote and develop security standards and verification mechanisms. For instance, the facility provides products and solutions testing and validation environment and platform for customers, including white-box and black-box type verification.

Continue to provide cybersecurity thought leadership by contributing to the cybersecurity ecosystem in all 170 countries and regions where Huawei operates, leveraging on leading cybersecurity events and social media platforms to engage and lead cybersecurity activities; and providing leadership in professional industry

Thought leadership presentation at major conferences for e.g. GISEC in Dubai, UAE

MoU signing ceremony to support the UAE ICT Academy and commitment to nurture 10,000 ICT professionals in 3 years

organisations in senior leadership position to deliver industry white papers, best practices, and standards, most often not, are made available for free for anyone to use. In fact, Huawei has joined more than 360 standards organizations, industry alliances, and open-source communities and held over 300 key positions, including board or executive committee membership, in the IIC, IEEE-SA, BBF, ETSI, TMF, WFA, OASIS, WWRF, OpenStack, Linaro, ONAP, IFAA, GP, CCSA, and AII. In 2018, Huawei submitted more than 5,000 standard proposals, increasing Huawei's total number of standard proposals to 54,000. Huawei also submitted 251 security standard proposals to the 3GPP SA Working Group (WG) 3.

Continue to invest in reducing the digital divide. Huawei believes that no one should be left behind in the digital world as the organization believe in using the technology, applications, and skills to empower people and organizations everywhere. As such we continue our partnerships with institute of higher learning and organize global ICT competition to hone and benchmark their skills.

2020 Achievements

Huawei continues to set the bar in terms of openness, transparency, and collaboration as it continues to operate in some of the toughest cybersecurity regimes in the world and being scrutinized harder than anyone else. The sixth annual report of the UK Oversight Board of the Huawei Cyber Security Evaluation Centre (**HCSEC**) is testimonial to that where Huawei came up top with improvement in multiple domains with a solid record in security where Huawei equipment have been running stably with no major cybersecurity incident in the last 30 years despite the tough operating environment globally.

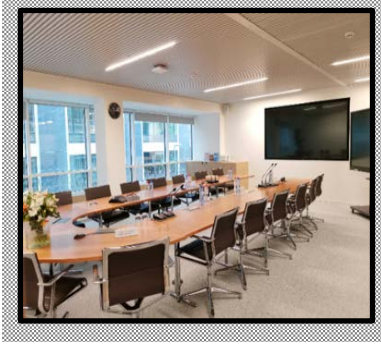
Huawei continue to provide thought leadership globally where we provide solutions that can be deployed with reference case studies as we grappled with a world that is crippled by Covid-19 amid the Industrial 4.0 revolution where governments globally are digitally transforming their countries, ironically accelerated by the work-from-home requirement brought about by the pandemic. For example, in the Middle East, Huawei has strengthened its commitment to the region's technology ecosystem through strong endorsement and participation in GITEX 2020. At GITEX, Huawei collaborated with partners from around the world to showcase how governments and organisations in the Middle East could create new values through synergy across five technical domains. Huawei had strengthened its commitment to the region's technology ecosystem where we confirmed our largest ever GITEX Technology Week presence at the 40th anniversary edition of the event in 2020. Huawei believes that connectivity, cloud, AI, computing, and industry applications are now truly coming together that will create unprecedented opportunities for society. As such, Huawei focuses on applying ICT technologies to more industries through scenario-specific solutions that help enterprises to enhance their business, and governments to achieve strategic goals related to domestic productivity and improving overall governance.

In line with Huawei's commitment to supporting the digital transformation vision of UAE, the organization announced a talent cultivation program to nurture 10,000 ICT talents over the next three years. At the back of this initiative, Huawei signed back-to-back agreements with multiple universities that will focused on building capabilities in these universities to support the '*seeds of the future*' vision. As part of this initiative, Huawei had recently held the first Innovation Competition in the Middle East where students used AI, cloud computing and big data to create valuable applications for the

society, with 10 university teams reached the finals.

Huawei Cybersecurity Transparent Centre in Shenzhen, China

Huawei Cybersecurity Transparent Centre in Brussels, Belgium



2021 Planned Activities

While continuing to play an integral part as a responsible and contributing member of the global cybersecurity ecosystem, Huawei have the following major key initiatives:

Promotion of an open standard on 5G security that is certifiable and acceptable worldwide. NESAS, jointly defined by 3GPP and GSMA, provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry. NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as using 3GPP defined security test cases for the security evaluation of network equipment. NESAS is intended to be used alongside other mechanisms to ensure a network is secure, an appropriate set of security policies covering the whole lifecycle of a network. The scheme should be used globally as a common baseline, on top of which individual operators or national IT security agencies may want to put additional security requirements. With 5G being much of an enabler in the Middle Eastern digital transformation narrative, it seems deem fit that a CERT organization with much influence in the region should take on the task to harmonize government 5G security standards and certification regime based on NESAS.

Pushing the envelope on cloud security where in the recent years have seen the rapid evolution of threats to cloud security, with new threats emerging at an alarming and increasing pace. The introduction of zero trust, and other applications that include deep technology such as IoT, Blockchain, AI and Big Data and the acceleration of digital transformation amidst Covid-19 create complications on the use cases.

Another cloud-related key activity planned is the development of a Cloud ISAC. While there was already IoT ISAC globally, but Cloud ISAC still remains as an idea first mooted by the Cloud Security Alliance, first called CloudSIRT, then CloudCERT and finally CloudCISC currently, which is a closed sharing platform surprisingly contrary to the spirit of building an open and transparent platform for information sharing. Hence, with the proliferation of cloud especially in the Middle East region, it seems fit that we can restart discussion to kick-start a cloud ISAC supporting National CERTs or government SOC, that focuses on being open and transparent that facilitate responsible information sharing under the control, management and supervision of a CERT organisation.

Finally, participate in the development of deep technology security guidance. Deep technology today, such as 5G (5G2B), AI, IoT, Blockchain etc. are still at the very early stage in terms of setting any security standards for them that can be accepted by all providers/vendors and governments. For example, even on 5G, applications of 5G on business application i.e. 5G to B or 5G2B would be the focal point for rollout into businesses as a replacement for setting up an intranet / internal network in a compound or site. What would be the recommend security guidance for such deployment?

In the pursuit to deliver these activities, we aim to work with the various standards organizations, industry alliances, and open-source communities and platforms such as GISEC / GITEX, which we have already been working with, to jointly work on these projects. Specifically, we will work closely with OIC-CERT to drive the realization of these projects and create good cybersecurity artifacts that will benefit the industry globally.

Turkcell CDC

(Cyber Defence Center of Turkcell)

Background

Turkcell is a converged telecommunication and technology services provider, founded and having a headquarter in Turkey. Turkcell CDC is the Cyber Defence Centre of Turkcell. Turkcell CDC provides a variety of services in the Information Security domain at national and international level including threat intelligence, managed security operations centre, and digital forensics & incident response services. Moreover, Turkcell CDC provides the Digital Security Service for individual Turkcell customers. With this service the customers are protected from various types of phishing and fraud attacks as well as credential leakage.

Turkcell CDC is part of the Turkcell Cyber Security Directorate which provides other services in the cybersecurity domain. These services are:

- sales, installation, and integration of network security products
- health check services for network security products
- penetration and DDOS tests and managed DDOS protection services

Establishment

Turkcell CDC is established in Dec 2015.

2020 Highlights

Summary of Major Activities

In 2020 Turkcell CDC launched multiple cybersecurity services to its enterprise and individual customers:

Turkcell CDC Digital Security Service

Digital Security Services

Turkcell Digital Security Service is a solution designed specifically for Turkcell's mobile Internet users. As phishing & fraud attacks continue to become more sophisticated, persistent, and adapt to mobile security defences, demand for phishing and fraud defence solutions is at an all-time high. Turkcell Digital Security Service encourage the users to connect only with safe endpoints. This service alerts users for any suspicious connection attempts or links with the help of machine learning and artificial intelligence algorithms. The service informs the customers, if they are using e-mail and social media accounts that have leaked passwords.

Threat Intelligence Service (Bozok)

Turkcell CDC has launched a threat intelligence platform named Bozok that provides up to date Indicator of Compromise (**IoC**) information, threat actor reports, data leakage detection, brand protection, and vulnerability detection services for the enterprise customers.

Digital Forensics and Incident Response Services

As a result of digital transformation, the trend shows the number of vulnerabilities and threats against information technology systems are increasing. Turkcell CDC Security Engineers are experts in their fields and can respond correctly and quickly to cyber incidents using industry standard methodologies. When faced with a cyber incident, Turkcell

CDC engineers effectively identify effected systems, complete the root cause analysis, determines all remediation actions, and assists customers get the effected environment back to a safe state.

2020 Achievements

In 2020, Turkcell renewed its ISO 27001 certification. Furthermore, Turkcell Cloud became the first cloud service provider in Turkey that is ISO 27017 certified. Turkcell CDC CTF teams attended multiple Capture the Flag events in 2020 and achieved high rankings. Some of these CTFs are: vShield CTF 1st place, First CTF 3rd place, Siber Yildiz 4th place. Finally, in 2020 Turkcell CDC became member of OIC-CERT and became an authorized user of Carnegie Mellon University's CERT Mark.

Activities & Operation

Events involvement

In 2020, Turkcell CDC increased its participation in virtual cybersecurity conferences with the start of Covid-19 Pandemic. Turkcell CDC members presented on various cybersecurity topics in ITU IEEE Com Week, vSheild, IDC, KVK and Bilisim Zirvesi conferences. Turkcell CDC attended the Turkish Cyber Security Cluster Week and gave three presentations on topics ranging from attack surface analysis to purple teaming. Also, in 2020 Turkcell CDC participated in Microfocus' virtual customer forum in which Turkcell CDC shared experiences regarding the state-of-the-art distributed ESM infrastructure.

Achievement

In 2020, Turkcell renewed its ISO 27001 certification. The Turkcell Cloud became the first cloud service provider in Turkey that is ISO 27017 certified. Turkcell CDC CTF teams attended multiple Capture the Flag events and achieved following rankings in 2020: '*vShield CTF*' 1st place, '*First CTF*' 3rd place, '*Siber Yildiz*' 4th place. Turkcell CDC became member of OIC-CERT and became an authorized user of Carnegie Mellon University's CERT Mark.

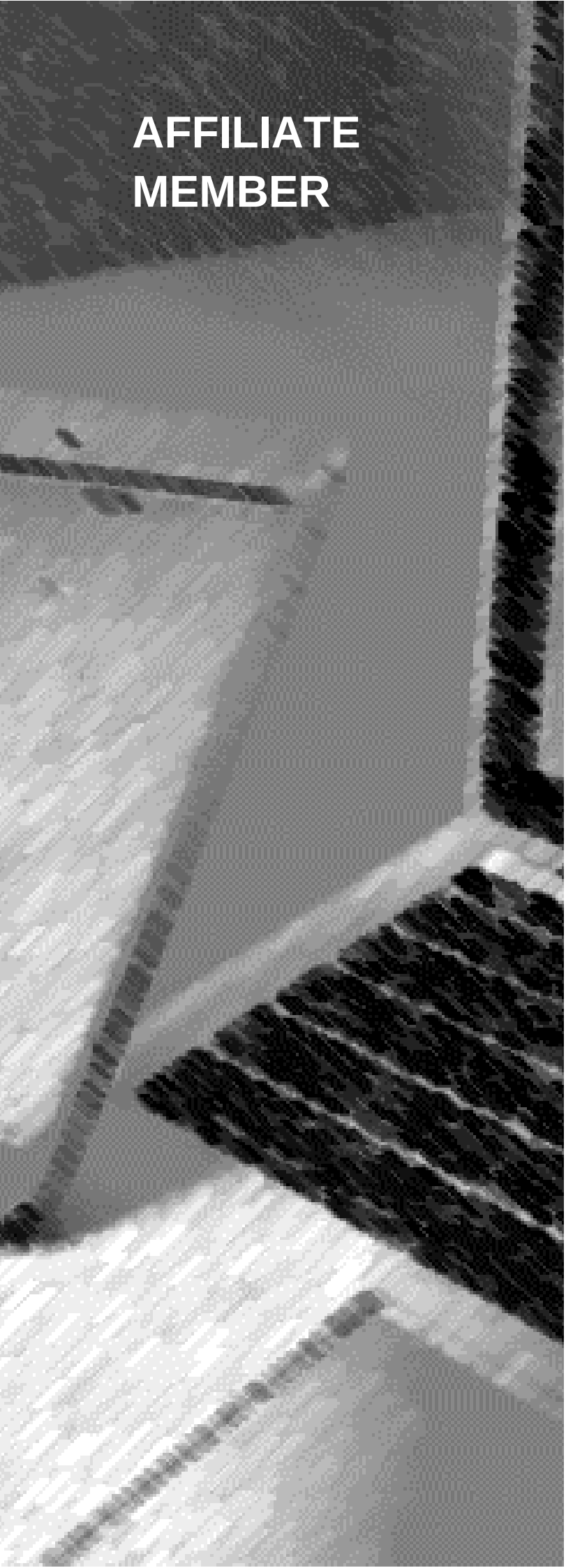
2021 PLANNED ACTIVITIES

Turkcell CDC is planning to hold a week-long cyber security training for University students called Cyber Camp in the spring of 2021.

Turkcell CDC is also planning to launch SOAR as a service model for its enterprise SOC customers in the first half of 2021.

Turkcell CDC Manager at National Cybercrime Conference 2020

Turkcell CDC member presentations at Cyber Security Cluster online conference



AFFILIATE MEMBER

Team CYMRU INC

Background

Since 2005, Team Cymru's mission has been to save and improve human lives by working with the public and private sector analyst teams, enabling them to track and take down threat actors, criminals, terrorists, and human traffickers around the globe.

Establishment

2005

Resources

Team Cymru is a private entity, debt free, and mission driven.

Constituency

Global, commercial, and community services.

2020 Highlights

Summary of Major Activities

Launch of Nimbus Threat Monitor Community Service in October 2020

Acceptance of member 133 to our CSIRT Assistance Programme - gmCSIRT – Gambia CSIRT

Activities & Operation

Events organized by the organization / agency

RISE-Finland 2020 – Team Cymru Regional Event

Team Cymru Annual Conference '*The Underground Economy 2020*' was cancelled due to the pandemic

Events Involvement

VB2020 presentation on '*Pandemic: Emissary Pandas in the Middle East*'

Team Cymru Dragon's Den Chat: Barry Greene (Trust Groups)

Sponsorship for the OIC-CERT Annual Conference 2020

Sponsorship for FIRST.org Annual Conference 2020

Achievement

34 blog postings at *team-cymru.com/resources/blog/*

New site for the configuration templates at *https://github.com/team-cymru/network-security-templates*

2021 Planned Activities

Release of UTRS 2.0 – Unwanted Traffic Removal Service

Release of MHR 2.0 – Malware Hash Registry

Release of versions 1.1 to 1.3 of Nimbus Threat Monitor

Team Cymru Annual Conference '*The Underground Economy 2021*'

Team Cymru Regional Event '*RISE-Colombia*' with LACNIC36

"...to save and improve human lives by working with the public and private sector analyst teams, enabling them to track and take down threat actors, criminals, terrorists, and human traffickers..."

PROFESSIONAL MEMBER

Dr. Abdulrahman Ahmad Abdu Muthana

(Smart Security Solutions)

Background

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

Establishment

Smart Security Solutions Company was established in October 2010 by Dr. Abdulraman Muthana and a group of information security professional.

Resources

Smart Security Solutions company includes several information security professionals and researchers. The company has two (**2**) training labs equipped with all the facilities and a research lab.

Constituency

Information Security fields.

2020 Highlights

Summary of Major Activities

Mobile banking applications penetration testing

Cybersecurity training

Network penetration testing

Security awareness program training

Ransomware incident investigations

2020 Achievements

Penetration testing of the mobile banking applications for local financial corporations

Penetration testing of network infrastructure for a local Bank

Security awareness training for local banks staffs

Secure coding training for two software development companies

Investigation of ransomware virus ".qlkm" attack incident

Activities & Operation

Events organized by the organization / agency

Information security training courses

Information security awareness training programs for employees of Yemen-Kuwait Bank - 13 Aug to 27 Dec 2020

Events involvement

Information security training

Information security awareness programs

Malware incidents analysis

Penetration testing

Achievement

Provide training on information security courses such as CEH and Certified Information Security Auditor (**CISA**)

Conduct information security awareness programs for the Management and users

Ransomware virus investigations

Penetration testing

2021 Planned Activities

Development of security plans, train staffs, and help financial corporations in Yemen to implement the ISO/IEC 27000 ISMS Standard

OIC-CERT Permanent Secretariat
CyberSecurity Malaysia (Malaysia)
An Agency Under the Ministry of Communications and Multimedia Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
secretariat@oic-cert.org
www.oic-cert.org