The OIC-CERT Annual Report 2019
About the OIC-CERT

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

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

Vision

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

Mission

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

Objectives

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

Encouraging the sharing of cybersecurity experience and information.

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

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

Promoting collaborative research, development, and innovation in cybersecurity

Promoting international cooperation with international cybersecurity organizations.

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

As of Dec 2019, the OIC-CERT has a network and strategic collaboration with 49 members from 27 OIC countries. This alliance is further supported through the presence of 3 Commercial Members, 4 Professional Members, 1 Fellow Member, 1 Affiliate Member, and 1 Honorary Member.

Full Members

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

1. Azerbaijan - Azerbaijan Government CERT (CERT.GOV.AZ)
2. Bangladesh - Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)
3. Brunei Darussalam - Brunei Computer Emergency Response Team (BruCERT)
4. Cote D’Ivoire - Cote D’Ivoire Computer Emergency Response Team (CI-CERT)
5. Egypt - Egypt Computer Emergency Response Team (EG-CERT)
6. Indonesia - Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (Id-SIRTII/CC)
7. Iran - Iran Computer Emergency Response Team (IRCERT)
8. Jordan - Jordan Computer Emergency Response Team (JO-CERT)
9. Kazakhstan - Kazakhstan Computer Emergency Response Team (KZ-CERT)
10. Kuwait - Kuwait National Cyber Security Center (NCSC-KW)
11. Kyrgyzstan - Computer Emergency Response Team of Kyrgyz Republic (CERT-KG)
12. Libya - Libyan Computer Emergency Response Team (Libya-CERT)
13. Malaysia - CyberSecurity Malaysia
14. Morocco - Moroccan Computer Emergency Response Team (maCERT)
15. Nigeria - Consultancy Support Service Limited (CS2)
16. Oman - Oman National Computer Emergency Response Team (OCERT)
17. Pakistan – National Response Centre for Cyber Crimes (NR3C)
18. Qatar - Qatar Computer Emergency Response Team (Q-CERT)
19. Saudi Arabia - Saudi Arabia Computer Emergency Response Team (CERT-SA)
20. Somalia - Somalia Computer Emergency Response Team (SomCERT)
21. Sudan - Sudan Computer Emergency Response Team (SudanCERT)
22. Syria - National Agency for Network Services
23. Tunisia - National Agency for Computer Security (tunCERT)
24. United Arab Emirates - UAE Computer Emergency Response Team (aeCERT)
25. Uzbekistan - Uzbekistan Computer Emergency Response Team (UzCERT)

General Members

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

1. Bangladesh
   - BangladeshCERT
   - Bangladesh Computer Emergency Response Team (bdCERT)
2. Iran
   - Isfahan University of Technology Computer Emergency Response Team (IUTcert)
   - Amirkabir University of Technology Computer Emergency Response Team (AUTcert)
   - Sharif University of Technology Computer Emergency Response Team (SharifCert)
   - Shiraz University ICT Center (SUcert)
   - Maher Center
   - APA Ferdowsi University of Mashhad CERT (APA-FUMcert)
   - APA University Bojnord CERT (APA-UBCERT)
3 Kazakhstan
   • Center for Analysis and Investigation of Cyber-Attacks (CAICA)

4 Malaysia
   • Universiti Teknikal Malaysia Melaka (UTeM)

5 Pakistan
   • Pakistan Information Security Association (PISA-CERT)

6 Turkey
   • Turkey Computer Emergency Response Team (TR-CERT)

7 Uganda
   • Uganda Computer Emergency Response Team (UG-CERT)

Affiliate Members

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

   The United States
   • Team Cymru

Commercial Members

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

1 South Korea

2 Singapore
   • CERT-GIB

3 Malaysia
   • FireEye Malaysia

Professional Members

1 Malaysia
   • Assoc. Prof. Hatim Mohammad Tahir - Universiti Utara Malaysia
   • Prof. Dr. Rabiah Ahmad - Universiti Teknikal Malaysia Melaka
   • Abdul Fattah Mohamed Yatim - Teknimuda (M) Sdn Bhd

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

Fellow Members

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

Tunisia
   • Prof. Nabil Sahli - National Agency for Computer Security

Honorary Members

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

   Saudi Arabia
   • The OIC
Members’ Report

Azerbaijan
   Azerbaijan Government CERT (full member) .............. 7

Bangladesh
   Bangladesh e-Government Computer Incident Response Team (full member) ........................................ 10

Brunei Darussalam
   Brunei Computer Emergency Response Team (full member) ................................................................. 14

Egypt
   Egypt Computer Emergency Readiness Team (full member) ....................................................................... 18

Indonesia
   National Cyber and Crypto Agency (full member) ................................................................................. 20

Iran
   Iran Computer Emergency Response Team (full member) ........................................................................... 23

Jordan
   Jordan Computer Emergency Response Team (full member) ..................................................................... 26

Kuwait
   Kuwait National Cyber Security Centre (full member) 28

Kyrgyzstan
   Kyrgyz Republic Computer Incident Response Team (full member) ......................................................... 30

Malaysia
   CyberSecurity Malaysia (full member) ....................................................................................................... 31

Oman
   Oman National Computer Emergency Readiness Team (full member) ..................................................... 39

Pakistan
   Pakistan Information Security Association (general member) .................................................................. 44

Saudi Arabia
   Saudi Arabia Computer Emergency Response Team (full member) .......................................................... 47

Somalia
   Somalia Computer Emergency Response Team (full member) .................................................................. 49

Sudan
   Sudan Computer Emergency Response Team (full member) .................................................................... 50

Tunisia
   National Agency for Computer Security (full member) .............................................................................. 52

United Arab Emirates
   UAE Computer Emergency Response Team (full member) ........................................................................ 54

Uzbekistan
   Uzbekistan Computer Emergency Response Team (full member) ............................................................ 59

Yemen
   Smart Security Solutions (professional member) ....................................................................................... 62

Group-IB
   Computer Security Incident Response Team Group-IB (commercial member) ........................................... 63
### Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCT</td>
<td>Arab Cybersecurity Cooperation Team</td>
</tr>
<tr>
<td>ACID</td>
<td>ASEAN CERT Incident Drill</td>
</tr>
<tr>
<td>ACSC</td>
<td>Australian Cyber Security Centre</td>
</tr>
<tr>
<td>AGM</td>
<td>Annual General Meeting</td>
</tr>
<tr>
<td>AITI</td>
<td>Authority for Info-communications Technology Industry</td>
</tr>
<tr>
<td>AJCCBC</td>
<td>ASEAN – Japan Cybersecurity Capacity Building Center</td>
</tr>
<tr>
<td>APCERT</td>
<td>Asia Pacific Computer Emergency Response Team</td>
</tr>
<tr>
<td>APIA</td>
<td>Asia Pacific Internet Association</td>
</tr>
<tr>
<td>APNIC</td>
<td>Asia-Pacific Network Information Centre</td>
</tr>
<tr>
<td>APRICOT</td>
<td>Asia Pacific Internet Conference on Operational Technologies</td>
</tr>
<tr>
<td>ARCC</td>
<td>Arab Regional Cybersecurity Centre</td>
</tr>
<tr>
<td>ASEAN</td>
<td>Association of South East Asian Nations</td>
</tr>
<tr>
<td>BSSN</td>
<td>Badan Siber dan Sandi Negara / National Cyber and Crypto Agency</td>
</tr>
<tr>
<td>CAMP</td>
<td>Cybersecurity Alliance for Mutual Progress</td>
</tr>
<tr>
<td>CBK</td>
<td>Common Body of Knowledge</td>
</tr>
<tr>
<td>CCDA</td>
<td>Certified Cyber Defender Associate</td>
</tr>
<tr>
<td>CCNA</td>
<td>Cisco Certified Network Associate</td>
</tr>
<tr>
<td>CDFFR</td>
<td>Certified Digital Forensic for First Responder</td>
</tr>
<tr>
<td>CEH</td>
<td>Certified Ethical Hacker</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CII</td>
<td>Critical Information Infrastructures</td>
</tr>
<tr>
<td>CIIP</td>
<td>Critical Information Infrastructure Protection</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td>CISAM</td>
<td>Certified Information Security Awareness Manager</td>
</tr>
<tr>
<td>CISMS</td>
<td>Certified Information Security Management System</td>
</tr>
<tr>
<td>CISSP</td>
<td>Certified Information Systems Security Professionals</td>
</tr>
<tr>
<td>CITC</td>
<td>Communication and Information Technology Commission</td>
</tr>
<tr>
<td>CIW</td>
<td>Certified Internet Web Professional</td>
</tr>
<tr>
<td>CNI</td>
<td>Critical National Infrastructure</td>
</tr>
<tr>
<td>CNII</td>
<td>Critical National Information Infrastructure</td>
</tr>
<tr>
<td>COP</td>
<td>Child Online Protection</td>
</tr>
<tr>
<td>CTF</td>
<td>Capture the Flag</td>
</tr>
<tr>
<td>CTRC</td>
<td>Cyber Threat Research Centre</td>
</tr>
<tr>
<td>CPT</td>
<td>Certified Penetration Tester</td>
</tr>
<tr>
<td>CSIRT</td>
<td>Computer Security Incident Response Team</td>
</tr>
<tr>
<td>CSAP</td>
<td>Certified Secure Application Professional</td>
</tr>
<tr>
<td>CSM-ACE</td>
<td>Cyber Security Malaysia – Award, Conference &amp; Exhibition</td>
</tr>
<tr>
<td>CSP</td>
<td>Cyber Secure Pakistan</td>
</tr>
<tr>
<td>CSRA</td>
<td>Cybersecurity Readiness Assessment</td>
</tr>
<tr>
<td>EGNC</td>
<td>E-Government National Centre</td>
</tr>
<tr>
<td>FIRST</td>
<td>Forum of Incident Response and Security Teams</td>
</tr>
<tr>
<td>GCFA</td>
<td>GIAC Certified Forensic Analyst</td>
</tr>
<tr>
<td>GCI</td>
<td>Global Cybersecurity Index</td>
</tr>
<tr>
<td>GCIA</td>
<td>GIAC Certified Intrusion Analyst</td>
</tr>
<tr>
<td>GCIH</td>
<td>GIAC Certified Incident Handler</td>
</tr>
<tr>
<td>GFCE</td>
<td>Global Forum on Cyber Handler</td>
</tr>
<tr>
<td>GIAC</td>
<td>Global Information Assurance Certification</td>
</tr>
<tr>
<td>GPEN</td>
<td>GIAC Penetration Tester Certification</td>
</tr>
<tr>
<td>GREM</td>
<td>GIAC Reverse Engineering Malware</td>
</tr>
<tr>
<td>GCSP</td>
<td>Geneva Cybersecurity Policy</td>
</tr>
<tr>
<td>GRF</td>
<td>Global Resilience Federation</td>
</tr>
<tr>
<td>CSRA</td>
<td>Cybersecurity Readiness Assessment</td>
</tr>
<tr>
<td>L</td>
<td>LEA</td>
</tr>
<tr>
<td>-----------</td>
<td>-----</td>
</tr>
<tr>
<td></td>
<td>LSN</td>
</tr>
<tr>
<td>M</td>
<td>MBOT</td>
</tr>
<tr>
<td></td>
<td>MCSA</td>
</tr>
<tr>
<td></td>
<td>MoU</td>
</tr>
<tr>
<td></td>
<td>MTCNA</td>
</tr>
<tr>
<td></td>
<td>MTCP</td>
</tr>
<tr>
<td>N</td>
<td>NAP</td>
</tr>
<tr>
<td></td>
<td>NCERT</td>
</tr>
<tr>
<td></td>
<td>N-CIRT</td>
</tr>
<tr>
<td></td>
<td>NCA1</td>
</tr>
<tr>
<td></td>
<td>NCA2</td>
</tr>
<tr>
<td></td>
<td>NCSC</td>
</tr>
<tr>
<td></td>
<td>N-SOC</td>
</tr>
<tr>
<td></td>
<td>NATO</td>
</tr>
<tr>
<td></td>
<td>NDC</td>
</tr>
<tr>
<td></td>
<td>NECTEC</td>
</tr>
<tr>
<td></td>
<td>NTRA</td>
</tr>
<tr>
<td>O</td>
<td>OIC</td>
</tr>
<tr>
<td></td>
<td>OIC-CERT</td>
</tr>
<tr>
<td></td>
<td>OJCS</td>
</tr>
<tr>
<td></td>
<td>OSCE</td>
</tr>
<tr>
<td>R</td>
<td>RBPF</td>
</tr>
<tr>
<td>S</td>
<td>SCNA</td>
</tr>
<tr>
<td></td>
<td>SCNP</td>
</tr>
<tr>
<td></td>
<td>SLA</td>
</tr>
<tr>
<td></td>
<td>SOC</td>
</tr>
<tr>
<td>T</td>
<td>TAIEX</td>
</tr>
<tr>
<td></td>
<td>TC</td>
</tr>
<tr>
<td></td>
<td>TF-CSIRT</td>
</tr>
<tr>
<td></td>
<td>TNAS</td>
</tr>
<tr>
<td></td>
<td>TVET</td>
</tr>
<tr>
<td>U</td>
<td>UAE</td>
</tr>
<tr>
<td></td>
<td>UK</td>
</tr>
</tbody>
</table>
Azerbaijan

Azerbaijan Government CERT (full member)

Background
Azerbaijan Government CERT - CERT.GOV.AZ offers expert assistance in computer and network security incident handlings. These are incident coordination functions for all incidents involving systems and networks located in the state sector of the Azerbaijan Republic.

More information can be found at:
Promo: https://www.youtube.com/watch?v=tYqPc-Izd54

Host Organization
- Special State Protection Service of Azerbaijan
- Special Communication & Information Security State Agency
- CERT.GOV.AZ

Establishment
- 20 April 2008

Resources
- Government

Constituency
All networks and the users in the state sector of the Azerbaijan Republic.

Contacts
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

2019 Highlights

Summary of Major Activities
- Incident Response
  CERT.GOV.AZ assist system administrators in handling the technical and organizational aspects of incidents. The organization will aid or advice 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 used vulnerability)
    - Facilitating contact with other sites which may be involved
Making reports to other CERT/CSIRT teams
Composing announcements to users, when applicable

**Incident Resolution**
- Removing vulnerabilities
- Liquidation of the consequences of incidents
- Evaluating of possible additional actions considering the cost and risk
- Aid in evidence collection and data interpretation when needed
- Collect statistics of the incidents and will notify the community where necessary to assist in protecting against known attacks

**Proactive Activities**
- Information services - CERT.GOV.AZ publishes advisories of events and incidents that are considered to have special importance to users in the constituency. The information is disseminated via various channels (web, RSS feeds, mailing lists etc).
- Training services - Members of the CERT.GOV.AZ periodically conduct seminars on various aspects of information and network security.

### 2019 Activities, Achievements & Events

- Recorded and handled 4447 incidents
- Provided 266 audit / penetration test for required government bodies
- Updated user list on OIC-CERT Awareness system and provided five (5) tests
- Updated required workflow in OIC-CERT Membership Portal
- Published new service - blacklist.gov.az to register domains that used in phishing attacks
- Conducted cybersecurity training for local and foreign banks that operates in Azerbaijan
- Published 3 series of “Information Security” journal for government bodies which are distributed for free
- Participated in the Malaysian Technical Cooperation Programme (MTCP)

### 2020 Planned Activities

- To publish multifunctional anti malware program on CyberWeek 2020 - [https://www.youtube.com/watch?v=eK_84ncWFEE](https://www.youtube.com/watch?v=eK_84ncWFEE)
- Plan to provide feeding portal for blacklisted domains with malware
- Work on OIC-CERT membership portal for updates
- Work on functionality to make a blacklist.gov.az service much more practical in use
- Continue collaboration with CERTs internationally

- Participated in various local and international conferences, meetings, and courses i.e. OIC-CERT, Forum of Incident Response Security Teams (FIRST), North Atlantic Treaty Organization (NATO), and Organization for Security and Co-operation in Europe (OSCE)
CERT-lerin təkmələyi: yeni trendlar və çağırışlar

tex.f.d., dün. Yədiqar İmamverdiyev
AMEA informasiya texnologiyaları institutu

Azərbaycan Milli Elmlər Akademiyası

OIC-CERT 2019 Annual Report
Bangladesh

Bangladesh e-Government Computer Incident Response Team (full member)

Background

The Bangladesh Government’s Computer Incident Response Team (BGD e-GOV CIRT) is acting as the National Computer Incident Response Team of Bangladesh (N-CIRT). Currently, the responsibilities include receiving, reviewing, and responding to computer security incidents and activities. Under the Government of people’s republic of Bangladesh, BGD e-GOV CIRT reviews and takes the necessary measures to resolve the issues 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 (LEAs), academia, and civil society to help improve the cybersecurity defences of Bangladesh.

Establishment

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

Resources

Currently, there are 13 staffs working in BGD e-GOV CIRT and it is expected that more will be joining soon.

Constituency

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 National CIRT of Bangladesh with a mandate to serve the entire country.

2019 Highlights

Summary of Major Activities

• 910 cyber security incidents registered in the tracking system

• Arranged 10 cyber security training / workshops

• Five (5) cyber sensor units deployed to CII

• Provided more than 15 digital forensic case report to several government organizations

• Developed self-assessment tool kit for cyber risk assessment for CII organizations

• Conducted risk assessments in CII organizations

• Developed and published Bangladesh Cyber Threat Landscape 2019

• The Cyber Range provided training to 100 Government officials in 2019

• Total of 5 major IT (information technology) audit activities completed successfully for 5 government organizations

• Provided monthly threat intelligence reports to several government stakeholders

• Published monthly cyber bulletins for the stakeholders

2019 Achievements

• Participated in the OIC Drill 2019

• The National Data Center (NDC) ISO 27001 re-certification audit successfully done under the supervision of the audit team and received the ISO 27001 certification
• Received the Task Force on Computer Security Response Teams (TF-CSIRT) accreditation certificate

2019 Activities & Operations

Events organized by the organization / agency:

• Conducted the Bangladesh threat landscape workshop for CII

• Arranged workshop on Cyber Range Operation for all government banks, the Bangladesh Air Force & Military Institute of Science & Technology of Bangladesh

• Conducted the training on Digital Forensics - Military Institute of Science & Technology of Bangladesh

• Conducted trainings on cybersecurity - Prime Minister’s Office, Bangladesh

• Conducted two (2) security awareness sessions for the NDC employees and a session for ISACA (Information Systems Audit and Control Association) local chapter

Events involvement

• Attended the 11th OIC-CERT Annual Conference 2019 conjunction with the 8th Regional Cybersecurity Summit and FIRST & ITU-ARCC Regional Symposium - Muscat, Oman 27–31 Oct 2019

• Participated in the International law in cyber space program - George C. Marshall European Centre for Security Studies, Germany

• Participated in the Program on Cybersecurity Studies" training - George C. Marshall European Centre for Security Studies, Germany

• Attended the International Workshop on Cybersecurity Education and Workforce Development Capacity Building - George C.
- Attended the 12th Annual Cyber Security Week 2019 - Colombo, Sri Lanka
- Attended the Black Hat Asia 2019 Conference - Singapore

Achievements

- Provided 60 cyber sensor analysis reports (from Jan 2019 to Dec 2019) to multiple CII
- 166 cyber security advisories and news have been published on BGD e-GOV CIRT website to bring awareness of cybersecurity to the people
- Actively providing social media monitoring report on suspicious activity detections which helps the government to secure the social media environment

3 weeks PCSS course, George C. Marshall, European Centre for Security Studies

Applicability of international law to state behaviour in cyber space course, George C. Marshall European Center for Security Studies, Germany
2020 Planned Activities

• Upgrade Cyber Risk Assessment Framework
• Perform risk assessment to CII
• Provide regular cyber sensor analysis reports (intrusion and suspicious activity) to CII where cyber sensors are deployed
• Provide training on the Industrial Control System (ICS) in the public sector
• Mobile applications penetration test
• ISO 20000 Certification for the National Data Center Tier-III
• Audit plan for eight (8) government organizations
Brunei Darussalam

Brunei Computer Emergency Response Team (full member)

Background

The Brunei Computer Emergency Response Team - BruCERT was established in May 2004. It was formed in collaboration with the Authority for Info-communications Technology Industry (AITI) of 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.

Services

- 24 x 7 security related incidents and emergency response onsite (deployment response is within two (2) hours after an incident is received.) This service only applies to BruCERT constituents.
- Broadcast alerts (early warning) of new vulnerabilities, advisories, viruses, and security guidelines from BruCERT website. BruCERT constituents will receive alerts through email and telephone as well as defence strategies in tackling IT security related issues.
- Promote security awareness program to educate and increase public awareness and understanding of information security and technical know-how through education, workshop, seminar, and training.

Establishment

BruCERT coordinates with the local and international CSIRTs, network service providers, security vendors, LEAs 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) where the majority specializes in IT while the rest are in administration and technical support. The staffs have undergone training in 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 (CISPP), BS7799 Implementer and SANS trainings such as the Global Information Assurance Certification (GIAC) certifications 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). This is where most of BruCERT workforce gained their certifications.

Constituents

BruCERT has established good relationship with government agencies, two (2) major Internet Service Providers (ISPs) 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 digital forensics 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 the government departments and ministries in Brunei Darussalam. Services such as the IT Central Procurement, Network Central Procurement, Co-location, ONEPASS (a PKI initiative), and Co-hosting are provided by EGNC. BruCERT works closely with EGNC in providing incident response and security monitoring since most of the government equipment resided in EGNC.

- **The Authority for Info-communications Technology Industry of Brunei Darussalam**

  The Authority for Info-communications Technology Industry of Brunei Darussalam - AITI is an independent statutory body to regulate, license and develop the local ICT industry and manage the national radio frequency spectrum. AITI has appointed the Information Technology Protective Security Services (ITPSS), an IT local security company, to become the national CERT and manage the cyber security incident responses in Brunei.

**Royal Brunei Police Force and other LEAs**

BruCERT has been collaborating with the Royal Brunei Police Force (RBPF) and LEAs to resolve computer-related incidents through BruCERT’s Digital and Mobile Forensics services.

**Contact**

BruCERT welcomes reports on computer security related incident. Any computer related security incident can be reported as follows:

Tel: +(673) 245 8001  
Fax: +(673) 245 8002  
Email: cert@brucert.org.bn  
reporting@brucert.org.bn  
Website:  
www.brucert.org.bn  
www.secureverifyconnect.info

**2019 BruCERT Operation**

**Incidents response**

In 2019, BruCERT had received a lot of reports from the public as well as from BruCERT security intelligent sensors. Malware infections are the most common cyber threats upon Brunei Darussalam, there are few cases involving ransomware and coinminer type of malware. The statistic of the security incident is shown by BruCERT Statistic 2019 diagram.

<table>
<thead>
<tr>
<th>Type of Attacks</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Service</td>
<td>2</td>
</tr>
<tr>
<td>Explained Anomaly Event</td>
<td>36</td>
</tr>
<tr>
<td>Investigating Events</td>
<td>62</td>
</tr>
<tr>
<td>Malicious Software</td>
<td>2243</td>
</tr>
<tr>
<td>Non-compliance Activities</td>
<td>1071</td>
</tr>
<tr>
<td>Reconnaissance</td>
<td>75</td>
</tr>
<tr>
<td>Root Level Intrusion</td>
<td>109</td>
</tr>
<tr>
<td>Unsuccessful Activity Attempt</td>
<td>61</td>
</tr>
<tr>
<td>User Level Intrusion</td>
<td>151</td>
</tr>
</tbody>
</table>

**BruCERT Honey Pot**

In 2019, the most attack services which were recorded by BruCERT HoneyPot sensors were Telnet services which are around 33,909,549 attacks. The grand total of attacks on services was recorded at 69,851,021. Refer to the figure and table on the following page for the details.
Event Type |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
</tr>
<tr>
<td>DSC</td>
</tr>
<tr>
<td>EPMAP</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>MYSQLDB</td>
</tr>
<tr>
<td>SIP</td>
</tr>
<tr>
<td>SMB</td>
</tr>
<tr>
<td>SSH</td>
</tr>
<tr>
<td>Telnet</td>
</tr>
<tr>
<td><strong>Total</strong></td>
</tr>
</tbody>
</table>

The most attack port recorded in 2019 is port number 1433, which is usually used by Microsoft SQL Server. It might be the work of a new variant of a worm, trying to infect the Microsoft SQL server.

Port | Count |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>3,128,284</td>
</tr>
<tr>
<td>23</td>
<td>11,306,678</td>
</tr>
<tr>
<td>53</td>
<td>572,979</td>
</tr>
<tr>
<td>445</td>
<td>74,382,643</td>
</tr>
<tr>
<td>1433</td>
<td>166,201,495</td>
</tr>
<tr>
<td>1900</td>
<td>27,573,036</td>
</tr>
<tr>
<td>3306</td>
<td>96,441</td>
</tr>
<tr>
<td>5060</td>
<td>24,918</td>
</tr>
<tr>
<td>12502</td>
<td>888,758</td>
</tr>
<tr>
<td>49160</td>
<td>1,403,095</td>
</tr>
</tbody>
</table>

BruCERT honeypot managed to capture some of the malware hashes. The following figure shows the summary of the most detected malware in BruCERT Honeypot.
Detected Malware type in BruCERT Honeypot

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic Trojan</td>
<td>47</td>
</tr>
<tr>
<td>Coinmine</td>
<td>237</td>
</tr>
<tr>
<td>Ransomware</td>
<td>238</td>
</tr>
<tr>
<td>Unknown</td>
<td>16</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>538</strong></td>
</tr>
</tbody>
</table>

**2019 Highlights**

**Seminars / Conferences / Meetings / Visits**

BruCERT attended and presented at various seminars, conferences and meetings on content related to the field of Information & Communication Technology (ICT) security.

- Three (3) BruCERT delegates attended the OIC-CERT AGM and Annual Conference 2019 hosted by OMAN CERT - Muscat, Oman, 27 - 31 Oct 2019
- Two (2) BruCERT delegates attended the APCERT AGM and Annual Conference 2019 hosted by the Singapore Computer Emergency Response Team - SingCERT - Singapore 29 Sep - 2 Oct 2019

**Awareness Activities**

- **Cyber Battle : Capture The Flag 2019 and Awareness Talk** – 3 Aug 2019

BruCERT/ ITPSS Sdn Bhd hosted the 5th Annual Cyber Battle: Capture The Flag (CTF), a hacking competition which aims to highlight the importance of cybersecurity, and the increasing need for information security specialists in Brunei.

The participants attempted to solve challenges in a variety of real-life scenarios, in a race against time to obtain the ‘flags’ and submit them to the CTF scoring server.

This year, for the first time, the competition was also open to solo participants.
Egypt Computer Emergency Readiness Team (full member)

Background
The 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 organization collaborate with the government and financial entities, and any other CII sectors within Egypt. EG-CERT mission is to provide an early warning system against the spreading of malwares and the massive attacks against the Egyptian CII.

Resources
- Incident handling
- Malware analysis
- Penetration testing
- Digital forensics
- Cyber security awareness

Constituency
The Egyptian National Telecom Regulatory Authority

2019 Highlights
Summary of Major Activities
- Regular incident handling within our constituency
- Malware analysis of various types of malware samples
- Performing penetration testing on our 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 16 cases

2019 Achievements
- Managed to prevent many incidents and mitigated the risk of several other critical incidents
- Managed to issue over 170 malware intelligence reports and to create removal tools for the malwares affecting our constituency
- Managed to patch many vulnerable critical systems under our constituency
- Held several awareness sessions for different entities in Egypt

Activities & Operation
Events organized by the organization / agency:
- In December organized the 1st national cybersecurity summit as part of the activities of the 23rd Cairo ICT Expo
- Organized the 1st national official CTF competition
- The awareness team was part of UEA5 (Upper Egypt In Action 2019)

Events involvement
- Both the summits and the CTF were fully organized by EG-CERT
- Participated in the UEA 5 sessions
Achievements

• All the events organized by EG-CERT were very successful
• The UEA event was also very successful
Indonesia

National Cyber and Crypto Agency (full member)

Background

The government agency which has national responsibility in cyber security started with the establishment of Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Centre - Id-SIRTII/CC, which is National CERT of Indonesia, on 4 May 2007 by Minister of Communication and Information Decree no 26 in 2007. From 2007 until 2018, Id-SIRTII/CC has a function as the National CSIRT and coordination centre for national incident handling and work under the Directorate of Telecommunication of the Ministry.

Based on Presidential Decree no 53 in 2017, Id-SIRTII/CC was merged and moved to the National Cyber and Crypto Agency (in Bahasa = Badan Siber dan Sandi Negara or BSSN). Since April 2018, this new national agency officially started with bigger responsibilities and strategic roles as the top-level authority for cybersecurity related activities in Indonesia. It is also directly under the President and the merging of two agencies which are ID-SIRTII/CC and National Crypto Agency (Lembaga Sandi Negara - LSN).

Establishment

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

Resources

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

Constituency

Ministries and Government Agencies, LEAs, National Defence, CII Operators, Cyber Security Communities, Internet Service Providers (ISPs), Network Access Providers (NAP), Local Internet Exchange Operator, other Sector CERT/CSIRT’s in Indonesia.

2019 Highlights

Summary of Major Activities

In 2019, Indonesia conducted a few activities related to cybersecurity such as improving the national cyber capacity as well as strengthening the collaboration and coordination, especially in term of CII sectors. Its achievement in the involvement and contribution in the region are maintained such as in ASEAN, Asia Pacific, OIC and other global forum.

Cyber Drill Test for government sector 2019

In terms of OIC-CERT, Indonesia had been elected as the Deputy Chair of OIC-CERT during the recent OIC-CERT AGM 2018 in Shiraz, Iran, while continuing with the second term as the Board Member. Its main role is to contribute to the capacity building programs together with Malaysia as part of the OIC-CERT strategic pillar.

Based on the national cybersecurity monitoring and incident report, there was no large-scale network security incident in 2019 that cause
massive damage, but it is very important to increase the attention level on issues affecting the CII. Thus, it is necessary for the government, ISPs, societies, internet users, to pay much more attention and to cooperate with one another more effectively. There is also the need to increase 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 threats.

2019 Achievements

The major achievement in 2019 is the re-establishment of Indonesia Gov-CSIRT - Gov-CSIRT.ID. Previously, the Gov-CSIRT.ID is under the Ministry of Communication and Technology. However, since the function of information security was positioned under BSSN, the re-launched of Gov-CSIRT.ID was done and put under the BSSN. The Gov-CSIRT.ID also introduces more services for their stakeholders, such as reactive services, proactive services, and quality management services.

Activities & Operations

Events organized by the organization / agency
- **Cybersecurity Drill** - Cyber drill for government agencies and CII sectors
- **Conferences and Seminars** – Forum of Incident Response and Security Teams Technical Colloquium (**FIRST TC**), Forum Group Discussion of Government Sector

Events involvement
- **AFCEA TOKYO TECHNET 2019** – Tokyo, Japan 5 – 7 Mar 2019
- Participated in the 2019 2nd ASEAN - Japan Cyber Security Working Group Meeting - Malaysia 23 – 24 Apr 2019
- Participated in 31st Annual FIRST Conference - Edinburgh 16 – 21 Jun 2019
- Benchmark to CNCERT/CC – **Beijing, China Jun 2019**
- Participated in Asia Pacific Computer Emergency Response Team (**APCERT**) 2019 Online Cyber Security Drill - **31 July 2019**
- Conducted the OIC-CERT Online Training Q3: **Social Engineering Framework** - Jakarta 3 Sep 2019
- Participated in the online ASEAN CERT Incident Drill (**ACID**) 2019 - 4 Sep 2019
• Participated in the OIC-CERT Annual Conference in conjunction with FIRST & the International Telecommunication Union – Arab Regional Cybersecurity Centre (ITU-ARCC) Regional Symposium for Africa and Arab Regions - Oman 15 Sep 2019

• Contributed as the FIRST-TC trainer for CSIRT training on Incident Response for Policy Makers during the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions - Oman 15 Sep 2019

• Participated in the MTCP - Malaysia 17 – 26 Sep 2019

• Participated as Speaker in OIC-CERT Academic Colloquium 2019 - Malaysia 24 – 27 Sep 2019

• Participated and Speaker in APCERT Annual General Meeting 2019 - Singapore 29 Sep – 2 Oct 2019

• Participated as a member in the OIC-CERT 11th Annual Conference 2019 - Oman 27 – 31 Oct 2019

15 Province Gov-CSIRT established. In addition, the ICT-ISAC was also running as the information sharing forum for CII in Telco operator/ICT sector, while the Financial Service/FS-ISAC is still under preparation.

2020 Planned Activities

In the year 2020, it is expected that Indonesia will have some new sector CERTs/CSIRTs that will be established especially in the local government sector for all regions as well as to conduct some capacity building activities on cybersecurity skills and CERT/CSIRT related management and incident response. In addition, the National Security Operation Centre (N-SOC) that will be the nationwide cyber security monitoring infrastructure is expected to be launched as well.

Achievement

Following the re-establishment of Gov-CSIRT.ID, Indonesia is now looking forward for some sector CERTs/CSIRTs that will be established especially in the local government (province) and CII related sectors. In 2019, there were already
Iran

Iran Computer Emergency Response Team (full member)

Background

The Iran Computer Emergency Response Team - IRCERT consist of information security teams that do assessing and analysing, monitoring, data gathering and updating, intrusion detection and incident response, maintenance, and support services. IRCERT receives vulnerability reports, software, and hardware products security flaws from the whole country, and provides IPs and ".ir" domains security.

Establishment

This centre is the single point in the Ministry of ICT for cyber space incident handling activities and coordination.

Resources

IRCERT is a vital subset of the Information Technology Organization (ITO) that is supported by the Ministry of Information and Communication Technology of Iran.

Constituency

This centre is part of the Security Deputy of Information Technology Organization - Ministry of Information and Communication Technology of Iran.

2019 Highlights

Summary of Major Activities

Under the name of CERT centres, Maher Centre began work as Iran's national CERT in 2008. Since then Maher Centre has the responsibility of country wide actions for the prevention of and response to security incidents in cyber space and information exchange environments.

- Immediate investigation of cyber space incidents and cybersecurity assistance
Discovering Vulnerabilities and Computer Security Statuses

Security evaluation of systems and Malware Analysis

Designing and developing tools and techniques to discover security threats and vulnerabilities

Publishing the latest cyber news

Organizing workshops and training classes in the field of cyber security

**2019 Achievements**

Discovering more than 6,000 malwares, attacks, and vulnerability throughout the country

Evaluating more than 2,000 security assessments

Providing security threats and vulnerabilities discovering tools such as:
  - Web based automatic security assessment system
  - Domain name system security.
  - Anti-phishing
  - DNS Automatic Security Test.
  - Intrusion Detection System - IDS penetration testing
  - Web based app penetration testing training system
  - Secure Sockets Layer - SSL checker
  - Honey net and vulnerability monitoring system
  - Distributed Denial of Service - DDoS resistance system

Establishing more than 500 news in Maher website

Publishing more than 300 reference cyber security documents

Holding training for cybersecurity classes and workshops for more than 40,000 hours

**Activities & Operations**

Events organized by the organization / agency:

- Holding International Iranian Society of Cryptology - ISC Conference on Information Security and Cryptology ISCISC’19- Sep 2019

- Holding workshops throughout the country
  - Malware analysis
  - Investigation novel cyber security defences
  - Security Operations Centres (SOC)
  - Object Security in Internet of Things (IoT)
  - governmental cyber security requirements
  - block chain
  - cyber security deep learning

- Holding training courses throughout the country
  - CCNA Security, Microsoft Certified Solutions Associate (MCSA), MikroTik Certified Network Associate (MTCNA)
  - Python Security
  - Penetration Test
  - Dark Web

**Events involvement**

- Attending the OIC-CERT face-to-face meeting - Cyberjaya, Malaysia

- Attending the OIC-CERT 11th Annual Conference in conjunction with The Regional Cybersecurity Week 2019 - Muscat, Oman

- Attending the 3rd Conference of CICA Non-Governmental Forum-Cyber Security – Chongqing, China
2020 Planned Activities

- Computer Security Incident Response Teams Reinforcement
- Training Expert CERT teams over the country
- Responding to malwares attacks
- Detecting and discovering zero day and important vulnerabilities. Pic 2: Block Chain Workshop
Jordan Computer Emergency Response Team (full member)

Background
The Mission of Jordan Computer Emergency Response Team - JoCERT is to protect the Hashemite Kingdom of Jordan’s public networks, data centres and critical infrastructure from cyber attacks.

Establishment
The Government of Jordan established JoCERT in 2018 to coordinate responses to computer security incidents within the government sector. The JoCERT will be operated under the umbrella of the Ministry of Digital Economy and Entrepreneurship.

Resources
- National Cyber Security Strategy 2018-2023

Cyber Security Law 2019

2019 Highlights

Summary of Major Activities
- Participation in local / international Cyber Security activities
- Conduct security awareness program to different levels of audience
- Enhance the capability of CERT operations

Achievements
- Respond to security incidents on national level
- Provide protection to national network and resources

Activities & Operation
Events organized by the organization / agency
- Participation in Cyber Shield 2019 – ITU Turkey Dec 2019
- Participation with National Center for Security and Crises Management in The Right Power Training – Oct 2019

- Participation in Certified Cyber Defender Associate (CCDA) training by CyberSecurity Malaysia – Sep 2019

Achievement
- Respond to state sponsored APT attacks that are targeting the Government infrastructure
- Enhance the capabilities to expand the visibility and increase the efficiency of daily operations
- Respond to around 500 incidents
- Build the capability to operate Vulnerability Management team
- Enhancement in the tools used for Malware analysis / Forensics

Education lectures for government institutions
- Holding educational lectures for government institutions
- Holding awareness lectures for schools affiliated with UNESCO entitled Safe Use of the Internet, where more than 3,500 students (male and female)
2020 Planned Activities

- Participation in local / international cybersecurity activities
- Improve the security awareness sessions and expand the targeted groups
- Enhance the threat intelligence feeds
- Participate in international cybersecurity forum such as FIRST
- Establishment of the Jordan Cyber Security Commission

Awareness lectures for schools
Kuwait National Cyber Security Centre
(full member)

Background
National Cyber Security Centre of the state of Kuwait - NCSC-KW is the body of all cybersecurity actions. After the publication of the National Cyber Security Strategy for the state of Kuwait 2017-2020, the centre took the responsibility to develop framework, operating model, and programme for the State of Kuwait focusing on main objectives as follows:

- Promote a culture of cyber security that supports safe usage of cyberspace
- Safeguard and continuously maintain the security of national assets

Establishment
A preparation phase (Phase 0) was conducted for 6 months period to define the cybersecurity maturity levels of the critical sectors in Kuwait.

- Enabling cybersecurity strategic visions to lead strategic implementations
- Implementing a risk management program
- Implement a strategic performance management program
- Manage cybersecurity agenda
- Situate and develop national cybersecurity main concerns
- Work in partnership with government agencies, companies, and institutions responsible for strategic implementation

Resources
Currently the Unit consists of few people however, we will recruitment as soon as the COVID-19 issue resolves.

Constituency
CITRA is the national CERT (NCERT) for the State of Kuwait.

2019 Highlights

Summary of Major Activities
Establish and promote a national cyber security structure including capacity development and awareness with all Critical National Infrastructure (CNI) to Secure Kuwait.

Achievements
- Cybersecurity awareness programme for CITRA
- Cybersecurity awareness for public
- Established cybersecurity major as diploma
- Organised the first research and education event in the field of cybersecurity
- Conduct several workshops and training for technical employees in the field of cybersecurity

Activities & Operation

Events organized by the organization / agency
- Cybersecurity Education & Research Conference
- Cyber Ops Certification Program Cisco CCNA training
- Threat Hunters Competition in partnership with ARCC
Events Involvement

- Cyber Warrior 2019 competition arranged by US Army
- Participation in the International Systems Security Certification Consortium – ISC2 Kuwait Chapter Meeting
- Participation in cyber security leaders program arranged by the Common Body of Knowledge (CBK)
- Participation in several trainings arranged by NATO school

Achievement

- NCSC Service to block inappropriate web content or apps online
- Information sharing platform within the Critical National Infrastructures (CNIs)

2020 Planned Activities

2020 is the year of implementation for Kuwait’s National Cyber Security Program. This program contains the National CERT (NCERT) as one of the 5 main pillars. The program provides the response and remediation activities in the areas of incident response, forensics, and red team, which will collaborate to achieve a fully functional national CERT supporting government departments and other high-level entities through an External Interface Management function. Moreover, the NCERT will join global CERT networks and continue to build and maintain relationships with the national and international CERTS. A continuation to study and assess national cyber security maturity levels and build and develop CERT employees’ levels of cybersecurity expertise in order to manage and handle the National CERT Programme.
Kyrgyzstan

Kyrgyz Republic Computer Incident Response Team (full member)

Background
The Kyrgyz Republic Computer Incident Response Team - CERT-KG is set up to improve standards and cybersecurity, as well as to protect IT infrastructure in the Kyrgyz Republic.

Establishment
CERT-KG was established in 2015.

Resources
Government

Constituency
CERT-KG constituency - all networks, information resources and users located in the field of information technology of the Kyrgyz Republic.

2019 Highlights

Summary of Major Activities
- Making proposals for the development of a cyber security policy
- Coordination of activities of organizations, centres for responding to computer incidents (departmental, industry and others) in order to ensure security and identify cyber security, identify, prevent, and suppress computer attacks, respond to computer incidents
- Identification, prevention and suppression of possible threats and cybersecurity
- Making suggestions for improving the legislation of the Kyrgyz Republic in the field of use and cybersecurity
- Participation in the development of international treaties of the Kyrgyz Republic in the field of security and cybersecurity
- Ensuring the fulfilment of obligations in the field of international relations, participation in which is carried out by the Kyrgyz Republic
- Accomplishment of tasks in accordance with regulatory legal acts of the Kyrgyz Republic

2019 Achievements

One of the main achievements is that CERT-KG was to become a full OIC-CERT member.

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
- ITU Regional Seminar for the CIS countries and Asia Pacific countries with the topic Cybersecurity - Sep 2019
- International Practical Forum Safety Positive Hack Days IX (9th) - Moscow Russia May 2019

2020 Planned Activities

- To establish a focal point in the field of cybersecurity
- To develop the first national cyber instructions
CyberSecurity Malaysia (full member)

Background

Establishment

CyberSecurity Malaysia (www.cybersecurity.my) was established with the formation of the Malaysia Computer Emergency Response Team - MyCERT on 13 January 1997 under the Ministry of Science, Technology and Innovation Malaysia. On 19 October 2019, CyberSecurity Malaysia was transferred under the purview of the Ministry of Communications and Multimedia Malaysia (Kementerian Komunikasi dan Multimedia Malaysia - KKMM). As a technical specialist agency, CyberSecurity Malaysia is committed to provide a broad range of cybersecurity innovation-led services, programmes, and initiatives to reduce the simultaneously strengthen Malaysia's self-reliance in the cyber space.

Specialised Services

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

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

CyberSecurity Malaysia’s scope of specialised cybersecurity services are as follows:

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

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 security issues based on the common international collaborative platforms and agreement.

2019 Highlights

- Participated in the Asia Pacific Internet Conference on Operational Technologies (APRICOT) & FIRST Technical Colloquium, organised by the Asia Pacific Internet Association (APIA), Asia-Pacific Network Information Centre (APNIC), and Korea Institute of Science and Technology (KISTI) - Daejeon, Korea 18 Feb 2019
- Participated in the Cyber Intelligence Asia 7th Annual Conference and Exhibition, organised by Intelligence-Sec Limited (UK) together with Thailand's National Electronics and Computer Technology Center (NECTEC) - Bangkok, Thailand 26 - 29 Feb 2019
- Hosted the OIC-CERT Board Face-to-Face Meeting 02/2019 - Cyberjaya, Malaysia 22 Apr 2019
- Organised the Cyber Security Industry Dialogue 2019 - Cyberjaya, Malaysia 23 Apr 2019
- Participated in the 4th Digital Forensics Expert Group Meeting - Sao Paolo, Brazil 22 - 25 May 2019
- Participated in the 6th ASEAN-Japan Cybersecurity Capacity Building Centre
Activities & Operations

Incident Handling Reports and Abuse Statistics

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

CyberSecurity Malaysia through MyCERT in 2019 has produced 18 advisories and 25 alerts to inform its 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/advisories2019

The following chart shows the reported incidents managed by CyberSecurity Malaysia for 2019.

Cyber Threat Research Centre

The Cyber Threat Research Centre (CTRC) operates a distributed research network for analysing malware and computer security threats. The centre has also established collaboration with trusted parties and researchers in sharing threat research information. Other activities of the centre include:

- 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 CERTs and international organisations
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. Till 2019, 7 issues of the Malware Trend Report have been published.

The project is using Lebahnet, which 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.

Online Trainings

CyberSecurity Malaysia organised 2 online trainings in 2019:

- Training on Handling Insider Threats was conducted by Associate Professor Dr. S.M Warusia from Universiti Teknikal Malaysia Melaka - UTeM. UTeM is one of the OIC-
CERT General Member. 102 participants took part in the training - 7 Mar 2019

- Training on Honeynet Data Analysis through LebahNet by Mr. Fathi Kamil Mohad Zainuddin. 71 participants took part in the training - 19 Jun 2019

Malaysian Technical Cooperation Programme

Malaysian Technical Cooperation Programme in progress

CyberSecurity Malaysia in collaboration with the Ministry of Foreign Affairs Malaysia successfully organised a training entitled Certified Cyber Defender Associate from 17-26 September 2019 under the MTCP.

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

In relation to this, the training program is structured to provide cybersecurity trainings for the participants focusing on enhancing relevant cybersecurity skills and operational capabilities specifically in the area of Security Compliance, Incident Handling, and Security Assessment.

The training program leveraged on state-of-the-art cybersecurity knowledge from domain experts and experience practitioners as well as through various collaborations with other subject matter experts.

Seventeen (17) participants from the following OIC-CERT and ASEAN countries attended the training:

- Azerbaijan (1)
- Egypt (2)
- Indonesia (2)
- Jordan (1)
- Kazakhstan (2)
- Lao PDR (1)
- Brunei Darussalam (2)
- Morocco (1)
- Myanmar (1)
- Nigeria (1)
- Oman (1)
- Philippines (2)
- Uzbekistan (1)
Global ACE Certification

The Global ACE Certification (www.cybereducationscheme.org) is a holistic framework of cybersecurity professional certification that outlines the overall approach, independent assessments, impartiality of examinations, competencies of trainers, identification and classification of cybersecurity domains, and the requirements of professional memberships.

The Global ACE Certification is developed in collaboration with the government, industry, and academia in Malaysia and supported by the OIC-CERT. The establishment of the scheme is in tandem with international standards such as ISO/IEC 9000 on processes, ISO/IEC 17024 on certification of persons and ISO/IEC 27001 on security management.

In Malaysia, the scheme is recognised by the Malaysia Board of Technologists (MBOT) through the Malaysia ACT 768 as a Professional Technologist or Certified Technician. The scheme is also recognised by the Department of Skill Development and MBOT under the Technical & Vocational Education Training (TVET) programme.

Global ACE Certification key achievements in 2019 are as follows:

- Six (6) professional training programmes conducted.
  - Certified Secure Application Professional (CSAP)
  - Certified Digital Forensic for First Responder (CDFFR)
  - Certified Information Security Management System (CISMS)
  - Certified Penetration Tester (CPT)
  - Certified Information Security Awareness Manager (CISAM)
  - Certified Cyber Defender Associate - CCDA

- One hundred and forty-three (143) participants attended the training programmes. Seventy-eight (78) participants passed the examinations and certified under the Global ACE Certification

- The first overseas Global ACE Certification examination conducted - Islamabad, Pakistan Jan 2019

- Seventeen (17) participants from various countries attended the Global ACE Certification training programmes through the MTCP Programme.

- Five (5) Knowledge, Skill & Attitude (KSA) 3.0 were developed
  - Penetration Tester
  - Secure Application Practitioner
  - Digital Forensics for First Responder
  - Intrusion Detection & Prevention Analyst

- Four (4) Knowledge, Skill & Attitude (KSA) 2.0 were developed
  - Incident Handling and Network Security Analyst
  - Data Security Analyst
  - Common Criteria Evaluator
  - IoT Security Analyst

- Eighteen (18) local universities/higher learning institutions interested and some have started aligning cybersecurity academic modules with the Global ACE Certification to incorporate professional credentials

OIC-CERT Journal of Cyber Security (Volume 2)

Malaysia under the OIC-CERT Business Plan – Capacity Building Pillar has established a platform for academia and cybersecurity practitioners to share their experiences and knowledge through research and publication. This initiative, the OIC-CERT Journal of Cybersecurity (OJCS), is published annually. In the recent publication, eight (8) papers were published and presented at the OIC-CERT Academic Colloquium in Kuala Lumpur, Malaysia.
International Collaboration

Malaysia’s National Cyber Security Policy identified international cooperation as one of the areas in enhancing cybersecurity. In line with this, CyberSecurity Malaysia is active in establishing collaborative relationships with foreign parties.

Visits

CyberSecurity Malaysia received working visits from several foreign organisations such as:

- Ministry of Transport and Infocommunications, Brunei
- Various agencies from Dong Nai Province, Vietnam
- Badan Siber Sandi Negara (BSSN), Indonesia
- Nation-Building Institute, Thailand
- Havelians, Turki

Memorandum of Understanding (MoU)

CyberSecurity Malaysia has signed MoUs with the following organisations for 2019:

- Gujarat Forensic Science University - India
- InterExchange Solutions Limited - Bangladesh.

International Roles

Among the international roles and contributions by CyberSecurity Malaysia are:

- The Permanent Secretariat of the OIC-CERT
- The Chair of the APCERT
- The convenor for the APCERT Malware Mitigation Working Group – addressing malware infections among the Internet users and cyber threat general issues. The main objectives are to provide an overview of cyber threats landscape due to malware 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 three (3) cross-national Cyber Drills in 2019 namely the APCERT Drill, the ACID Drill, and the OIC-CERT Drill.

As in the previous years, CyberSecurity Malaysia was involved in co-organizing international cyber drills for the OIC-CERT. In 2019, Malaysia collaborated with Oman in organising the drill with the theme, *The Rise of Malware Intelligence*. The objective of this drill is to get a more 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 as follows.

<table>
<thead>
<tr>
<th>OIC-CERT</th>
<th>APCERT</th>
<th>Africa CERT</th>
</tr>
</thead>
<tbody>
<tr>
<td>CERT.GOV.AZ</td>
<td>CERT-In</td>
<td>CERT-Mu</td>
</tr>
<tr>
<td>(Azerbaijan)</td>
<td>(India)</td>
<td>(Mauritius)</td>
</tr>
<tr>
<td>BGD e-GOV</td>
<td>Sri Lanka</td>
<td>RISA/Rw-</td>
</tr>
<tr>
<td>CERT</td>
<td>CERT/CC</td>
<td>CSIRT</td>
</tr>
<tr>
<td>(Bangladesh)</td>
<td>(Sri Lanka)</td>
<td>(Rwanda)</td>
</tr>
<tr>
<td>BruCERT</td>
<td>Eg-CERT</td>
<td></td>
</tr>
<tr>
<td>(Brunei)</td>
<td>(Egypt)</td>
<td></td>
</tr>
<tr>
<td>BSSN</td>
<td>JOCERT</td>
<td></td>
</tr>
<tr>
<td>(Indonesia)</td>
<td>(Jordan)</td>
<td></td>
</tr>
<tr>
<td>Eg-CERT</td>
<td>CyberSecurity</td>
<td></td>
</tr>
<tr>
<td>(Egypt)</td>
<td>Malaysia</td>
<td></td>
</tr>
<tr>
<td>JOCERT</td>
<td>maCERT</td>
<td></td>
</tr>
<tr>
<td>(Jordan)</td>
<td>(Morocco)</td>
<td></td>
</tr>
<tr>
<td>CyberSecurity</td>
<td>CS2 Limited</td>
<td></td>
</tr>
<tr>
<td>Malaysia</td>
<td>(Nigeria)</td>
<td></td>
</tr>
<tr>
<td>maCERT</td>
<td>PISA-CERT</td>
<td></td>
</tr>
<tr>
<td>(Morocco)</td>
<td>(Pakistan)</td>
<td></td>
</tr>
<tr>
<td>CS2 Limited</td>
<td>TunCERT</td>
<td></td>
</tr>
<tr>
<td>(Nigeria)</td>
<td>(Tunisia)</td>
<td></td>
</tr>
<tr>
<td>PISA-CERT</td>
<td>CERT-In</td>
<td></td>
</tr>
<tr>
<td>(Pakistan)</td>
<td>(India)</td>
<td></td>
</tr>
<tr>
<td>TunCERT</td>
<td>CERT-Mu</td>
<td></td>
</tr>
<tr>
<td>(Tunisia)</td>
<td>(Mauritius)</td>
<td></td>
</tr>
</tbody>
</table>

Achievements

Recognitions

CyberSecurity Malaysia actively participated in international cybersecurity events and has received recognitions as below:

- Accredited by INTERPOL for the contribution and assistance of digital forensics expertise in developing the *INTERPOL Global Guidelines for Digital Forensics Laboratories* during the
Research Papers

CyberSecurity Malaysia actively contributed research papers to journals and conference proceedings. Some of the papers are as follows:

- A Systematic Review on Cloud Security Auditing - published in Institute of Institute of Advanced Scientific Research
- Finding Annihilator(s) via Fault Injection Attach (FIA) on Boolean Function of Grain v0 - published in EDP Sciences
- Towards Implementing Scalable and Reconfigurable SCADA Security Testbed in Power System Environment - published in Inderscience Online
- A Comparative Analysis Study: Open Data Concepts in Smart Cities - published in IRAJ Publisher
- Terrorism Indoctrination via Social Media: A Malaysian Case Study - published in Academic Conferences and Publishing International Limited
- Man-in-the-Middle Attacks on Electrical Power Grid SCADA System - published in IEEE Xplore Digital Library
- Enhanced Automated-Scripting Method for Improved Management of SQL Injection
- Development of Denial of Service Mitigation for Internet of Things Sensor Node - Published in Global Academy of Training & Research
- Smart Energy Monitoring System for Residential in Malaysia - published in Association of Computing Machinery
- A New Cryptojacking Malware Classifier Model Based on Dendritic Cell Algorithm - published in Hong Kong Society of Robotics and Automation
- Malware Classification for Cyber Physical System (CPS) Based on Phylogenetics - published in Blue Eyes Intelligence Engineering & Science Publication
- Mobile Malware Classification Based on Phylogenetics - published in Blue Eyes Intelligence Engineering & Science Publication
- Android Malware Classification Using XGBoost On Data Image Pattern - published in IEEE Xplore Digital Library
- Enhanced Statistical Analysis Evaluation Using CSM Randomness Test Tool - OJCS Technical Colloquium

Penetration Tests on a Large Scale - published in IEEE Xplore Digital Library
2020 Planned Activities

CyberSecurity Malaysia strives to improve service capabilities and encourage local Internet users to report cybersecurity incidents to the MyCERT 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.

The human capital professional development is one of CyberSecurity Malaysia investment to the staff. CyberSecurity Malaysia will relentlessly encourage its staff to obtain certifications in cybersecurity. In addition, staff are encouraged to attend certification trainings, give presentations, and write publications at local and international platforms. This will assist them to improve their contribution in knowledge and experience sharing in the cybersecurity field. The staff are also encouraged to develop in-house tools used in mitigating security threats to assist the public and industry to secure and utilise their assets when performing online activities.

In 2020, some of key activities that CyberSecurity Malaysia will pursue are:

- To continue to work together with the local and international organisations through the establishment of formal relationship arrangements such as MoUs and Agreements
- To organise national events such as the CSM-ACE, which is an annual event providing awareness, training, and awards to information security professionals. In addition, the National ICT Security Discourse will be conducted to boost the cybersecurity awareness among the youth
- To co-organise international events such as the OIC-CERT Annual Conference
- To promote submission of manuscripts for publication in the OJCS (Volume 3). In addition, the OIC-CERT Academic Colloquium will be organized during the OIC-CERT Annual Conference
- To spearhead collaboration with other international partners and organisations. With such understanding, CyberSecurity Malaysia supports newly established local and international CSIRT by providing advice and assistance especially in becoming members to international information security community such as the APCERT, FIRST and OIC-CERT
Oman National Computer Emergency Readiness Team (full member)

Background

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

Resources

- CNII Protection team
- Cyber Security 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 Center team

2019 Highlights

Achievements

- ITU-ARCC have established the national CERT for Palestine - 24 – 28 Mar 2019
- ITU-ARCC participated as partner with ITU in delivering capacity building at the National Cybersecurity Strategy Workshop for Indonesia and ASEAN countries - Jakarta, Indonesia 26 -28 Aug 2019
- ITU-ARCC participated, developed and delivered a cyber-security scenario for the ITU Regional Workshop for Africa and Arab on “National Cybersecurity Strategies from - Tunisia 10 – 13 Dec 2019
- ITU-ARCC organized the national cybersecurity competition Threat Hunters for Oman, Lebanon, Kuwait, Egypt, Tunis, Sudan, and Palestine
- ITU-ARCC participated, developed, and delivered a cyber-security scenario for ITU Asia Pacific & CIS Inter-Regional Cyber Drill - Kuala Lumpur, Malaysia 23-27 Sep 2019
- Organized the regional cybersecurity competition Threat Hunters for seven Arab countries
- Organized the regional cybersecurity week 2019 in Sultanate of Oman including 7 events:
  - 8th Regional Cybersecurity Summit
  - 7th Regional Drill 2019
  - 7th Arab Cybersecurity Cooperation Team (ACCT) Meeting
  - FIRST Symposium
  - FIRST Training
- 11th OIC-CERT annual Conference 2019
- OIC-CERT Board Meeting No. 5/2019

ITU-ARCC participated in Oman National CERTs best practices paper in the National Cybersecurity Summit 2019, - 2 – 3 Dec 2019, Egypt

Signed 2-partnership agreement with cyber security industry

International Level

- OCERT chaired the OIC-CERT Board Meeting No. 5/2019 - 30 Oct 2019, Muscat, Sultanate of Oman
- OCERT chaired OIC-CERT Board Meeting No. 2/2019 - 22 Apr 2019, Kuala Lumpur, Malaysia
- OCERT chaired the meeting of ITU-T SG17 Regional Groups for Africa and Arab - 2 – 3 Apr Tunisia 2019

- OCERT awarded in the Middle East Award for Government Security Leaders
- Oman National CERT discovered a second security vulnerability in Apple - iOS

- OCERT participated as Strategic Partner in the National Cyber Drill – Muscat, Sultanate of Oman 9 – 11 Sep 2019
- ITU-ARCC in partnership with BSI have conducted the IRCA certified ISO/IEC 27001 ISMS Lead Auditor training program - 28 Apr – 2 May 2019, Muscat, Sultanate of Oman

OCERT chaired the ITU-T Study group 17 meeting - Geneva 25 Aug – 5 Sep 2019
- ITU-ARCC conducted Ethical Hacking training - Kyrgyzstan 19 – 22 Nov 2019
- OCERT received CISO MAG Summit & Awards Middle East

- 7th ACCT Meeting for Arab Region

Cyber security cooperation and alliances

- Signed 2 Partnership agreements with local / international industry partners as part of the partnership development program
- Collaborated with OIC-CERT to host the annual OIC-CERT Conference

- Oman National CERT hosted the OIC-CERT Cyber Drill 2019
- Collaborated with the global organization and FIRST to host a symposium and workshop for Middle East and Africa regions
Facilitated the membership of OIC-CERT for Somalia CERT, The Kyrgyz Republic (CERT-KG), and Uganda CERT as Full Membership. As for private sector we have facilitated Team Group IB (CERT-GIP), and Ernst & Young

Initiated collaboration with the Humanitarian Dialogue Centre (HD) and Geneva Cybersecurity Policy (GCSP) in Geneva on cybersecurity capacity building and cybersecurity concerns confronting the region and the various means being used to tackle them

Conducted a work for Omani investors on the world economic Forum report on Incentivizing Secure and Responsible Innovation

Activities & Operation

Cyber Incident and Services Management

Discovered and handled 483,794 real attempted service attacks, (152,480 web attacks, 152 malware attacks, 89,505 mobile attack and 2,099,498 phishing attacks) through OCERT Intelligence Gathering System resulted from the analysis of millions of attempted attacks against Oman cyber space

Successfully and comprehensively responded to 1,779 real cyber security incidents reported by the government, Critical National Information Infrastructures (CNIIs) and the public

Published 109 Security Threat Notification and Alerts (TNAS) on cybersecurity threats to OCERT constituents

Handled 162 digital forensics cases with 813 evidence devices including computers, mobiles, phones, external hard disk, and USBs resulted from cyber-crime cases in Oman

Successful integrated the national cyber early warning system with AI and international feeds

Data collection

Developed process model using artificial intelligence and machine learning to gather, measure, and normalize feeds from countless different sources based on attack types, which leads to reduced capacity storage of collected data feeds.

Data forecasting

Developed predictive models using machine-learning algorithms that look for trends and predict future attacks changes.

Government website monitoring

Developed a systematic government website monitoring that is using machine learning and integrated with our early warning system to produce automated alert notification system.

Developed 5 advanced cyber security scenarios executed in the ITU - Cyber Drills (Malaysia & Cyprus), OIC - Cyber Drill, the National Cyber Drill, and the Regional Cyber Drill.

Palestine CERT

The establishment which includes:

- the development of two different systems (incident management ticketing system, CERT portal and CMS)
- delivered CERT technical operation training
• developed customized penetration testing tool kit
• deployed mailing list system

CERT Implementation for Palestine

Cyber Security Professional Services
• Organized the National Cyber Drill for Government and CNII entities with participation from 73 organizations
• Cyber Security Ambassador Program:
  o Cybersecurity ambassadors have participated in threat hunter competition organized by OCERT
  o 75 new cyber security ambassadors joined the OCERT ambassador program total cyber security ambassadors are 783 – Public 221, Academia 365, Professional 196

Unified Government Information Security Campaign “WAAY”:
• 8 cyber awareness sessions were conducted under the program of the Information Technology Authority (ITA) Awareness sessions for each division on ITA
• 13 Awareness sessions in different government organizations, attended by 577 people
• Organized Cybersecurity Train the Trainer workshop for Government and CNII entities with participation from 42 organizations and attended by more than 63 people

Child Online Protection (COP):
• Participated in ITA kids’ event
• Participated in Shoukum session focused on child online protection
• Conducted 3 sessions on Child Online Protection Awareness 3 schools
• Participated in the Science festival
• Conducting CTF competition for 45 students
• Conducting Cyber Youth Talk (Cyber security workshop presented by students)
• Registration for junior cyber security ambassador program (around 112 new junior ambassador)
• Prepared the COP national strategy framework
• Prepared the COP situational analysis report
• Prepared the COP program business plan
Specialized Training:
- Conducted ISO 27001 lead auditor training attended by (19 people)

National Cybersecurity Campaign
- Target: Different segments
- Topics:
  - COP
  - Blackmailing
  - Financial crimes
  - Ethical hacking
- Tools:
  - 4 Radio interview.
  - 4 Articles
  - Participated in Shurkum session about child online protection
  - Covered MTC/CERT social media channels

Others:
- Participated in Youth Forum (during the Muscat festival)
- Participated in the Muscat festival
- Participated in COMEX
- Participated in Insight Cybersecurity Convention
- Participated in the Youth and Digital World Forum
- Organized Oman participation in Safer Internet Day
- Organized CNI CEOs Cyber-Security Seminar
- Regional Cybersecurity Week 2019, Oman
- Oman celebrating The Safer Internet Day 2019
- Regional Threat Hunter Winners Award 2019
Pakistan

Pakistan Information Security Association (general member*)

Background

The Pakistan Information Security Association - PISA is a not-for-profit organization working in the information security domain at different levels nationally and internationally. PISA is working with all the relevant stakeholders from the public and private organizations for the educational and 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

Resources

- Digital Forensics
- Cybersecurity
- Penetration Testing
- Incident Handling and Responses

Constituency

Pakistan

2019 Highlights

Summary of Major Activities

- Cyber Secure Pakistan 2019 – 12 Mar 2019
- Premium Seminar on Cyber Security in The Era of Emerging Technology – 6 Apr 2019
- Hands-On workshop on the theme of Investigating a Cyber Attack thru Splunk - 30 Aug 2019
- Cyber Secure Pakistan 2019, Lahore Episode – 31 Aug 2019
- Participated in the Global Cyberlympics - 7 Sep 2019
- OIC-Cyber Security Drill 2019 - 17 Sep 2019
- Cyber Secure Pakistan 2019, Peshawar Episode – 26 Sep 2019
- Seminar on Cyber Security 2019- 22 Oct 2019
- Cyber Threat Intelligence Day | International Conference – 24 Oct 2019
- Cyber Security Conference – 7 Nov 2019
- Margalla Dialogue on Peace and Development in South Asia, Middle East, Central Asia (SAMECA) – 13-14 Nov 2019
- PISA represented Pakistan CICA Conference in China - 18 Dec 2019
Activities & Operations

Events organized by the organization / agency:

- Cyber Secure Pakistan 2019 – 12 Mar 2019
- Premium Seminar on Cyber Security in The Era of Emerging Technology – 6 Apr 2019
- Cyber Secure Pakistan 2019, Lahore Episode – 31 Aug 2019
- OIC-Cyber Security Drill 2019 - 17 Sep 2019
- Cyber Secure Pakistan 2019, Peshawar Episode – 26 Sep 2019

Events involvement

- Represent Pakistan by participating in the Global Cyberlympics - 7 Sep 2019
- OIC-Cyber Security Drill 2019 – 17 Sep 2019
- Cyber Threat Intelligence Day | International Conference – 24 Oct 2019
- Seminar on Cyber Security 2019 – 22 Oct 2019

Achievements

In 2019, PISA has successfully completed the following targets:

- Organized seminars and workshops on cybersecurity in Universities / Government organizations
- Took part in the International Cyber Drills and Cyberlympics
- Supported in organizing the National Level Cyber Drills in Pakistan
- Successfully organize Cyber Secure Pakistan (CSP) main event in Islamabad as well as in other cities of Pakistan

2020 Planned Activities

- Planned to perform in International Cyber Drills
  - OIC Cyber Drill
  - APCERT Cyber Drill
- Planned in-house cyber drills for banks / universities / government organizations in Pakistan
- Seminars / Workshops
- Cyber Secure Pakistan (CSP) Main Events.
- Planned to participate in the National and International competitions (CTF / CyberLympics)
Saudi Arabia

Saudi Computer Emergency Response Team (full member)

Background

Saudi Computer Emergency Response Team’s - Saudi CERT 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 also launches awareness programs and campaigns, and cooperates and collaborates, with other response teams.

Establishment

Saudi CERT was established on the 1st of January 2006 by the Communication and Information Technology Commission (CITC). In October 2017, the National Cybersecurity Authority (NCA1) was established by a Royal Decree that involved transferring the CERT from CITC to NCA1.

Resources

- Incident Management team
- Incident Response team
- Digital Forensics team
- Information Sharing team
- Cybersecurity Assurance team
- Threat Monitoring and Hunting team
- Cybersecurity Awareness team
- International Coordination team

Constituency

Saudi CERT centre is part of NCA1 of the Kingdom of Saudi Arabia.

2019 Highlights

Summary of Major Activities

Saudi CERT seeks to raise cybersecurity awareness levels for citizens and organizations by raising the cybersecurity awareness programs. Saudi CERT provides services that facilitate:

- The management and release of cybersecurity alerts
- Cooperation with similar organizations
- Launching national programs that demonstrate the importance and dangers of cybersecurity
- Releasing cybersecurity awareness materials that describe the most prominent risks and best practices to prevent and mitigate these risks to enhance national awareness

These efforts will enable the cybersecurity community in the Kingdom of Saudi Arabia to become more resilient and agile when dealing with cybersecurity risks and attacks

Activities & Operation

Events involvement

- DNS Hijacking Drill - Dubai 16 April 2019
- The 31st Annual FIRST Conference - Edinburgh 16 - 21 Jun 2019
- The 14th Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT) - Edinburgh 21 – 22 Jun 2019
- The 8th Regional Cybersecurity Summit - Muscat 27 - 28 Oct 2019
- FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions - Muscat 29 Oct 2019
• The 11th OIC-CERT Annual Conference - Muscat 29 Oct 2019
• The 7th Regional Cyber Drill ALERT - Muscat 30 - 31 Oct 2019

2020 Planned Activities

• Hosting the Global Cybersecurity Forum (GCF)
• Instituting two global cybersecurity initiatives:
  o Save Children in Cybersecurity
  o Women Empowerment in Cybersecurity
• Hosting the 9th Regional Cybersecurity Summit
• Nominating to host the 12th OIC-CERT Annual Conference
• Establishing number of National Cybersecurity Awareness Program

Achievements

• Established Cybersecurity Awareness Campaigns with different topics targeting different categories - Children, Educators, Elderly, Employees, etc
• Ranked 13th among 175 countries in the Global Cybersecurity Index (GCI)
• Joined FIRST with full Membership

• Covered more than 12K vulnerabilities in the published security warnings
• Published more than 900 security warnings for entities and individuals
• Published Saudi CERT official website
Somalia

Somalia Computer Emergency Response Team (full Member)

Background

The National Computer Emergency Response Team in Somalia - SomCERT is one of the functions of the Cybersecurity Department at the National Communications Authority (NCA₂) to assess, analyse, and prevent incidents from cyber threats and attacks. One of the mandates of the SomCERT is to co-ordinate attack information and provide support for cyber incidents.

Establishment

SomCERT was established in the late 2019, to protect the public and private networks (ICT and Telecom Sectors) and the National Critical Infrastructures. SomCERT acts as a national CERT in Somalia.

Resources

SomCERT will provide incident response services (reactive, proactive, and security quality management services) to the public and private entities in Somalia soon.

Constituency

- Government entities
- Banks and Finance
- ISP
- ICT and telecommunication providers
- Energy and Water
- Academia

2019 Highlights

Summary of Major Activities

- The NCA₂ had established the SomCERT and joined as a Full Member of the OIC-CERT
- SomCERT developed policies, guidelines, and procedures
- SomCERT developed the Cybersecurity Readiness Assessment (CSRA) for the public and private sectors
- SomCERT developed an in-house training plan for 2020 for the staffs
- SomCERT participated in international workshops and conferences, such as the Global Forum on Cyber Expertise (GFCE) and GCI.

Achievements

- Establishing the National CERT Center
- Engaging stakeholders
- Developing basic documents
- Developing in-house training plan for 2020
- Developing the CSRA

2020 Planned Activities

- Conducting CSRA workshops
- Conducting National Cyber Security Awareness Campaigns
- Engaging national and international collaborations
- Participating in international cybersecurity workshops, training, and conferences, such as ITU and OIC-CERT
Sudan

Sudan Computer Emergency Response Team (full Member)

Background

Sudan Computer Emergency Response Team - Sudan CERT is a national ability to enhance information and network security all around Sudan.

- Serve as a trusted point of contact
- Response to computer security incidents
- Conduct security analysis (incidents, vulnerabilities, risks, etc)
- Encourage and promote a community of national and regional teams that share data, research, response strategies, and early warning notifications
- Participate in cyber “watch” functions
- Help organizations and institutions within the nation to protect their own networks

Vision: For a Safe Online Community.

Mission: To protect Sudanese citizens against the risks of Information Networks Including Internet.

Establishment

Sudan CERT is an initiative of the National Telecommunications Corporation – Sudan Telecom Regulatory Authority. Officially announced in 2010 and committed by ITU in 2013.

Resources

- Make general information security best practices and guidance available through publications and websites
- Promote security education, awareness, and training
- Provide vulnerability assessment service for web sites and organizations networks
- Monitor and control SPAM
- Provide technical advisories in network Security
- Promote COP programs

Sudan CERT is considered the official centre to provide the police with technical information regarding cyber crimes.

Constituency

- Government and private sector
- Universities
- Research Centres

Activities & Operation

- Events organized by the organization / agency
- A workshop in Strategies for Critical Infrastructure Systems Protecting - 1-3 Dec 2019
- Organizing the Threat Hunter Competition for 30 online competitors from other Arab countries under the auspices of ARCC

Events involvement

- Government sectors
- Private sector
- Universities and schools
- Talented students
- The prosecutors
- Digital community

Achievement

- Working group committee for CIP
- Knowledge & training
- Good awareness and brochures
2020 Planned Activities

- Project to build a national cybersecurity strategy
- CERT centre development
- Encouraging universities to establish incident response centres
- Rehabilitation and development of the digital evidence lab
- Obtaining the best technologies in the field of malware analysis and threats that targeting critical infrastructure systems i.e. SCADA, DCs, ICs
- Protecting the community from the negative effects of internet usage
- Contribute to the dissemination of informative guidance and guidance towards the safe uses of the technology
- Spreading a culture of COP in Sudanese society
- Monitor and follow up serious threats
- Developing a rapid response system to counter the increase in the number of cyber crime and information incidents
- Constructive international cooperation in cyber-security
**Background**

The National Agency for Computer Security - TunCERT carries out general supervision over computer systems and networks appropriate to the diversified public and private organisations.

**Establishment**

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

**Resources**

75 employees.

**Constituency**

National: private and public.

**2019 Highlights**

**Summary of Major Activities**

- Final stage of the follow-up with the Center of Informatics of the Ministry of Health to implement a Health Care CERT. Noting that a joint decision was signed between the two institutions to assign a working team to follow up with the project's implementation, provided that the exploitation will start from January 2020. This sector centre has been named CERT for health care.

- Final meeting before launching the Health Care CERT

- Holding meetings with representatives of the National Center of Informatics in the context of preparing for the establishment of a CERT-Administration

- Workshop on Protection of Bioinformatics Infrastructures' to raise the level, the degree of resilience, and the resilience of bioinformatics infrastructures against various cyber attacks

- Working sessions with representatives of the Tunisian Post to discuss the focus on detection of attacks and link it to the Saher system

- In collaboration with IEEE Tunisian Chapter, conduct a workshop under the theme "AI, Big Data, and Cybersecurity"

**Achievements**

- Launch the 1st mobile application dedicated to raise children's awareness on the risks and dangers to which they are exposed on the internet

- Signing of the national cybersecurity strategy
Activities & Operation

Events organized by the organization / agency:

- Organised the sectorial cyber drill to consolidate the reactivity of participants to face cyber attacks

- Organised the National Cyber Drill in collaboration with the National Center for Technologies in Education

- Organised a seminar with the theme "The Resilience of Information Infrastructures" which has a vital importance in collaboration with the technical assistance and information exchange instrument of the European Commission (TAIEX)

- Workshop organized ITU, in collaboration with the National IT Security Agency and in partnership with the ARCC and Deloitte as well as the Tunisian National Tourist Office, on the theme "National Cybersecurity Strategies"

Achievement

- Signing a partnership agreement with the High School of Communications of Tunis Sup'Com to launch the professional master's degree in Operational Cybersecurity

- Sponsoring of the first private Tunisian CSIRT, CSIRT.tn, to be a member of FIRST

2020 Planned Activities

- Health care CERT
- Administration CERT
- OIC-CERT AGM
- ITU National Cybersecurity Strategies
United Arab Emirates

UAE Computer Emergency Response Team (full Member)

Background

The National Computer Emergency Response Team - aeCERT launched several initiatives aiming to raise cybersecurity awareness and activate all initiatives that would spread awareness among different groups of society towards the importance of cybersecurity. aeCERT has been established to improve information security standards and practices, protects, and support UAE ICT infrastructures from online risks and breaches, and build a secure and protected ICT culture. aeCERT's 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.

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

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

aeCERT services cover:

- Governmental and semi-governmental entities
- Some of the private entities (especially banks)
- The public
- Academic institutions

Contacts

aeCERT welcomed reports on computer security related incident. Any computer related security incident can be reported at:

- Telephone: 800 12 (Toll Free)
- Facsimile: (971) 2 6118209
- Email: info@aecert.ae
- Website: www.aecert.ae
2019 Highlights

Summary of Major Activities

- Computer emergency response services
  - 343 cyber incidents addressed
  - More than one (1) million malware countered
  - 69 cybersecurity awareness documents issued

- Cybersecurity awareness services
  - 186 awareness sessions provided
  - 4698 people attended awareness sessions
  - 30 awareness videos published through the media
  - 12 security reports published
  - 23 cybersecurity ambassadors trained

- Information quality services
  - 79 vulnerability reports prepared
  - 30 vulnerability assessment testing
  - 48 penetration testing services

- Strengthen the Cyber Crime Law and assist in introducing new laws

- Raise information security awareness across the UAE

- Build national expertise in information security, incident management and computer forensics

- Provide a central trusted point of contact for cybersecurity incident reporting in the UAE

Achievements

Cybersecurity Strategy

- Cybersecurity Strategy Initiative in cooperation with McKinsey & Company. In 2018, aeCERT started building and developing a comprehensive cybersecurity strategy to be launched in 2019. The strategy is based on a document that includes standards for ensuring information security in the UAE and international standards pertaining to information security and protection.

- The team also conducted various baseline studies worldwide covering 11 countries that implemented information security and protection strategies.

- Conducting interviews and meetings with leaders and managers in information security and protection

Cybersecurity Strategy Implementation Manual

A strategy implementation guide and documents will be released during the first and second quarters of 2020.

Strategic projects for information security and protection:

- Critical Information Infrastructure Protection (CIIP) program management
- Implementing the national framework to support and accelerate the establishment of cybersecurity companies
- Implementing the national cybersecurity awareness strategy
- Implementing the cybersecurity capacity-building program
- Conference program and cybersecurity awards
Implementing the national framework program for cybersecurity legislation

National Framework for Cybersecurity Accreditation and Certifications

Follow up the national computer emergency plan

Develop regulations to support the implementation of the national computer emergency plan

Activate local and international partnerships

**Activities & Operation**

Events organized by the organization / agency.

* Gulf Information Technology Exhibition - GITEX

* Handling Internet Identifiers Abuse and Misuse Workshop

**Events involvement**

* **FireEye Cyber Defence Live**
  Co-organizing a technical summit with FireEye (FireEye Cyber Defence Live Summit).

* **ARCC Regional Cybersecurity Summit**
  TRA participates in the Regional CyberDrill in Oman.

* **Gartner Security & Risk Management Summit**
  Participating in panel discussion on cybersecurity strategy.

* **Digital Warfare**
  Participating in a workshop on cybersecurity strategy.

* **Cybersecurity In diplomatic work**
  Participating in a workshop on Cybersecurity in Diplomatic Work. Emirates Diplomatic Academy, in collaboration with Prince Saud Al Faisal Institute of Diplomatic Studies, organized a workshop on the impact of cybersecurity on the diplomatic work. During the workshop, the speakers discussed several topics including cyber crimes, norms, and laws on an international level. In addition, the workshop discussed cyber incidents, threats, and the attack landscape. aeCERT participated with a paper on the best strategies to combat international cyber threats.

* **IEEE UAE Cyber Intelligence Summit**
  Organize and participate in the Institute of Electrical and Electronics Engineers (IEEE) Summit, where the aeCERT team showcase the smart system for testing government applications.

* **Cyberbullying Panel Discussion (Etisalat)**
  Participating in the national week on cyber bullying with awareness sessions, activities, and capacity building workshops for families and government officials.

* **Cyber crimes (Shj Police)**
  aeCERT have participated in referent multimedia like television and radio live interview. Received questions from different social ages like children, adults, and seniors. Each category has its own needs and technological usage. Therefore, the responses are based on their understanding.

* **Cyberbullying Panel Discussion**
  Cyber-bullying conference is about the risk in having such threat in the community. The conference aims to spreads knowledge among parents and their children on how to deal with cyber-bullying.
Achievement

Key aeCERT projects.

SecureGCC
A system developed for CERTs of Arab Gulf states with the following features and capabilities:

- A secure way to share advisories, risks, and security information
- Cybersecurity processes and operations of the library
- Information leakage control system

TRUSTae
A system developed to automate vulnerability testing of systems and websites without human intervention by aeCERT members. It can be used by federal organizations and authorities in the UAE.

- Increase website/service quality and security tested by the system
- Minimize service delivery time

Source code review initiative
An aeCERT initiative to enable programmers and systems developers to test source code to ensure it is free of vulnerabilities.

VDR reporting initiative
An initiative by aeCERT aiming to provide proactive reports of security vulnerabilities in UAE federal government websites, thus reducing the number of security vulnerabilities, mitigating the risk of cyberattacks in the UAE and providing cost savings to entities.

Phishing assessment initiative
The initiative aims to enable entities to test the percentage of security awareness among their employees, especially through emails, where the aeCERT sends an email to the respective organization to collect employee data, provided that an awareness session for employees participating in the initiative is to be conducted at a later time.

Online awareness system initiative
This initiative aims to transform the current process of providing online awareness sessions into an electronic, automated method. The initiative aims to accommodate the largest number of attendees in addition to providing online awareness workshops for all categories of employees.

Cybersecurity ambassadors
This initiative aims to train several 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

Cybersecurity experts’ initiative
The initiative aims to develop aeCERT employee skills by providing a coach who assesses the skills of all team members, in addition to developing a schedule to train staff on the required skills.
• Increase employees’ skill
• Minimize training time
• Presenting a leading coach to provide experts with the leadership skill set required to steer teams

JIRA task management system
An electronic technical system that aims to develop the process of following up the tasks and responsibilities in the team along with providing a comprehensive view to the management of completed and current tasks of the team.
• Facilitate team communication
• Ensure aeCERT’s best compliance with the Service Level Agreement (SLA)
• Provide a task library and an enhanced method for following-up

aeCERT WIKI
An electronic system that serves as a library of procedures, processes, and best practices in aeCERT.

2020 Planned Activities

Cyber101
An initiative to train citizen IT staff on IT security and basics of cyber security. For federal entities, local authorities, student, and amateurs. The training will be monthly for 3 days.

CyberPro
A series of free monthly courses on cybersecurity to enhance the expertise of cybersecurity specialists and increase their readiness to address cyber risks.
• Beneficiaries
  o Cyber security specialists
  o IT and computer science specialists
  o University students
  o Anyone interested in cybersecurity
• Cyber Security week
National Cybersecurity Awareness week is a collaborative between the Telecommunications Regulatory Authority (TRA), government and private entities to raise awareness about the importance of cybersecurity in the country.

Cyber7
A national conference specializing in cybersecurity. Discusses cybersecurity issues and developments in practical ways and attracts cybersecurity experts from all over the world. Duration 6 days.
Uzbekistan

Uzbekistan Computer Emergency Response Team (full Member)

Background

The Uzbekistan Computer Emergency Response Team - UZCERT service, operating as a structural unit of the State Unitary Enterprise “Cybersecurity Center”, is focused on cooperation and interaction with operators and providers, as well as users of the national segment of the Internet, in providing the necessary support in responding to cybersecurity incidents. 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.

Establishment

The increased attention to the issues and problems of cybersecurity is associated with the approval of the Strategy for the Further Development of the Republic of Uzbekistan, aimed at the implementation of five (5) major strategic initiatives, which include security in the field of cybersecurity (Resolution of the President of the Republic of Uzbekistan dated February 7, 2017). The tasks of implementing government initiatives in the field of information and cybersecurity were assigned to the Information Security Centre created in 2013, which years later, following the government decision in 2019 was transformed into the State Unitary Enterprise Cybersecurity Center along with an increase in its role as responsible executive of state policy in the field of information and cybersecurity.

Resources

Government.

Constituency

UZCERT constituency - all networks, information resources and users located in the national segment of the Internet network of the Republic of Uzbekistan.

2019 Highlights

Summary of Major Activities

UZCERT is an incident response and cybersecurity service, which is a structural unit of the State Unitary Enterprise Cybersecurity Center. One of the main tasks is to reduce the level of security risk for users of the Uzbek national segment of the Internet. For these purposes, the UZCERT service provides access...
to domestic and foreign legal entities and individuals in the detection, prevention and suppression of illegal activities directed against information systems and resources of the UZ domain.

Achievements

- Collaboration with ITU and the computer incident response service of Japan, JPCERT/CC, which sponsored the UZCERT team, the status of a participant in the Suguru Yamaguchi Fellowship Program FIRST International Forum
- Joining the membership (status “listed”) of the Computer Security Incident Response Task Force, facilitating cooperation and coordination between the CSIRT in Europe and neighbouring regions TF-CSIRT, in consequence of assistance received from the Polish Emergency Response Computer Group - CERT Polska and the Latvian Information Security Incident Response Institute - CERT.LV
- Participation of the Centre’s delegation at the invitation of the President and Director General of KISA of the Republic of Korea in the 4th annual meeting of the Cyber Security Alliance in mutual progress and the seminar of the Global Center for Cybersecurity Development (the 4th Annual Meeting of the Cybersecurity Alliance for Mutual Progress - CAMP) and The Global Cybersecurity Centre for Development Seminar) where the CAMP Secretariat has officially announced that the Center has become a member of the CAMP operational committee
- The participation of the centre’s delegation in October 2019 at the OIC-CERT General Meeting and Annual Conference, where the main theme of the event “Regional Cybersecurity Week 2019” was the coverage of threats, evolution, opportunities and problems of cybersecurity in the 4th industrial revolution
- Assisting the Group-IB company (Russian Federation) as part of its entry into the OIC-CERT membership, as a sponsor. One of the main achievements is that UzCERT has become a full member of the OIC-CERT

Activities & Operation

Events organized by the organization / agency

State Unitary Enterprise Cybersecurity Centre regularly holds various seminars and training course on various enquiries and issues of information and cybersecurity for designated staff members of government bodies and institutions.

Events Involvement

In order to improve their qualifications, during 2019 the designated staff members of the State Unitary Enterprise “Cybersecurity Center” underwent training at various courses in the field of information and cybersecurity, such as:

- Group-IB (Russian Federation) in the field of digital forensics
- CyberSecurity Malaysia in the direction of information security
• **International CyberShield 2019** at the cybersecurity incident response exercise - *Turkey Dec 2019*

• **Positive Hack Days** (Russian Federation) during exercises on penetration tests on various devices

• **CERT.LV** in participated in the **Cyberchess 2019** international conference on cybersecurity - *Oct 2019*

• **Belt and Road Initiative** (People’s Republic of China), at seminars on information and innovative technologies and their protection

• Within the framework of the **6th International Internet Conference** (6th World Internet Conference, People’s Republic of China), at seminars and lectures on various topics on information technology, and participated in many foreign forums, which contributes to the further development of international relations in the Republic of Uzbekistan in the field of information and cybersecurity

### 2020 Planned Activities

Currently, the State Unitary Enterprise - Cybersecurity Centre is actively working on the coordination and signing of MoUs between the Centre represented by the UZCERT service and other foreign departments and organizations acting as CERT services. Among the countries with which agreements have been reached on further joint activities including the CERT Teams from the following countries - Republic of Kazakhstan; Poland, the Russian Federation, the UAE and Japan, as well as with private companies developing anti-virus software, such as KasperskyLabKz and Dr.Web.

To continue to develop cooperation with foreign partners.
Yemen

**Smart Security Solutions** (professional member)
Dr. Abdulrahman Ahmad Abdu Muthana

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

**Establishment**
SMARTSEC was established in October 2010 by Dr. Abdulrahman Muthana and a group of information security professionals.

**Resources**
SMARTSEC includes several information security professionals and researchers. The company has two (2) training labs equipped with the necessary facilities in addition to a research lab.

**Constituency**
Information Security fields.

**2019 Highlights**

**Summary of Major Activities**
- Malware Incident Investigations
- Research in Access Control
- Research in Android Security
- Information Security Training
- Supervising number of Information Security projects
- Security Awareness Program Training

**Achievements**
- Submitted an article entitled *Identity-Division Multiplexing Technique for Enhancing Privacy of Paging Procedure in LTE* to OIC-CERT Journal of Cyber Security
- Penetration Testing of Money Exchange system for a local Bank
- Investigation of Fingerprint Attendance System abuse incident, Government Corporation
- Investigation of Health Information System access violation incident
- Investigation of Ransomware virus " .devil" attack incident

**Activities & Operation**

**Events organized by the organization / agency**
- Information Security Training
- Seminar on Information Security Research for Post Graduate students
- Security Awareness Training for employees of Yemen-Bahrain Bank – 3-6 Nov 2019, 17-20 Nov 2019, 8-11 Dec 2019

**Events involvement**
- Information Security Training
- Information Security Awareness Programs
- Malware Incidents Analysis

**Achievement**
- Provide trainings of several information security courses
- Conduct several information security awareness programs
- Unified Extensible Firmware Interface (UEFI) Malware Investigation

**2020 Planned Activities**
- UEFI Malware Investigation
Group-IB

Computer Security Incident Response Team Group-IB (commercial member)

Background

In 2011 Group-IB established its CERT-GIB which became the first 24/7/365 computer security incident response team in Eastern Europe.

CERT-GIB is officially authorised by the Carnegie Mellon University (PA, USA) and licensed to use the "CERT" trademark in its name.

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

Establishment

10 Mar 2011

Resources

Human proficiency

- 60,000+ hours of emergency incident response
- Strategic team with a global vision, able to adjust defence methods to different verticals
- Close collaboration with the Digital Forensics Lab, Threat Intelligence and Cyber Investigation teams

Intelligence-driven

- Use of world-class proprietary threat intelligence
- Context analysis to foresee sophisticated cyber threats behind trivial events
- Development of cutting-edge solutions to improve cybersecurity practices

In-depth expertise in APTs

- Attribution of targeted attacks vs. random infections
- Identification of threats behind "legitimate" actions

International cooperation

- Partnership with CERTs and anti cybercrime associations worldwide striving to ensure safety in the digital space around the world
- Collaboration with all Russian top level domains which helps CERT-GIB block dangerous websites in these domains

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.
2019 Highlights

Summary of Major Activities
- Digital Forensics and Incident Response
- Cyber Investigations
- Threat Intelligence and Attribution
- Threat Hunting
- Security-Related information dissemination
- International cooperation with other CERT/CSIRT teams
- Cybersecurity awareness events and courses

Achievements
- Suspended work of 14093 phishing resources
- Signed memorandum of understanding in Cybersecurity field with UZ-CERT
- Became a member of the OIC-CERT
- Published annual Hi-Tech Crime Trends 2019/2020 threat report
- Participated in International CyberEx CTF
- Opened SOC in partnership with NGN International - Bahrain
- Opened Global HQ - Singapore
- Held Group-IB’s trademark threat hunting and intelligence conference CyberCrimeCon - Singapore and Moscow
- Notified CERT teams of other countries about incidents related to their government platforms (or associated resources)
- Got extended competencies in regional GeoTLD zones (such as .MSK.RU, .GEORGIA.SU and etc.) from FAITID
- Conducted an information security awareness campaign at international universities and schools
- Signed a MoU with the Institute of Technical Education - Singapore
- Signed a MoU with Ngee Ann Polytechnic - Singapore
- Signed a Partnership Agreement with Airome Technologies
- Published a whitepaper about mobile forensics services, data extraction methods, and case studies
- Published the whitepaper about the evolution of ransomware, its distribution, and the tactics and techniques used by APT groups
- Published the eDiscovery whitepaper about digital traces and how these traces can be detected
- Published the report Crime without punishment: in-depth analysis of JS-sniffers
- Published the report Malicious activity in H1 2019
- Published publicly available technical analysis of Silence’s tools, tactics, and evolution.
- Joining the “Ecommerce Foundation” alliance
Activities & Operation

Events organized by the organization / agency

- Cyber Security Workshop by NGN International & Group-IB - Manama, Bahrain Mar
- SOC launching event - Manama, Bahrain Apr
- Group-IB CyberDay - Innopolis; Kazan, Russia 18 Jun
- Group-IB Welcome Day - Singapore 18 Jul
- CyberCrimeCon 2019 - Moscow Russia 3 Oct
- Threat Day Group-IB - Amsterdam, Netherlands 12 Nov
- Group-IB Security Day - Almaty, Kazakhstan 14 Nov
- Group-IB CyberDay Skolkovo - Moscow, Russia 29 Nov

Webinars

- Take the next step in your Threat Intelligence program - 8 Feb
- Red Team versus Pen Test: how to build a better defence against advanced actors? - 19 Feb
- Incident Response Preparedness: a hard look at the statistics - 26 Mar
- How to investigate a perfect cybercrime? Tips & Tricks from Group-IB’s high-profile cases - 30 May
- How to level-up on your cyber knowledge: Group-IB Hands-On CyberSecurity Programs - 7 Jun
- How to safeguard your business from social engineering attacks? - 24 Jun
- Top-3 the most popular fraud schemes 2019 - 29 Jul
- Silence: Tools & Attack Evolution in 2019 - 9 Sep
- Are you ready for Cyber Incident Response? Expectation vs Reality - 10 Sep
- Evolving cyber threats in the Asia-Pacific region: How to track the most powerful hacking groups? - 19 Sep
- Gain Visibility to Phishing Infrastructure and Targets Affected - 12 Nov
- Analysis of Automated Lateral Movement Techniques Used in the Wild - 28 Nov
- Malware analysis: analysis of real cases - 5 Dec
- Hi-Tech Crime Trends 2019-20 - 6 Dec
- Proactive Hunting and Response - 10 Dec
- How to investigate corporate crime - 12 Dec
- New trends of fraudulent schemes in attacks on brands - 12 Dec

Events involvement

- SOC Forum Kazakhstan - Astana, Kazakhstan 18 Apr
- Security and protection of the Business. Innovations 2019 - Tbilisi, Georgia 19 Apr
• Cup of Reverse 2019 - St. Petersburg, Russia 23 Apr
• CTF ACISO (Association of Chief Information Security Officer) - Ekaterinburg, Russia 27 Apr
• CTF Bauman Moscow State Technical University - Moscow, Russia 12 May
• Cyber & Digital Security 2019; Nur-Sultan, Kazakhstan - 16 May
• Positive Hack Days 9; Moscow, Russia - 21 May
• Jet Security Conference - Moscow, Russia 6 Jun
• Threat Day with Anomali - Paris, France 4 Jun
• Malware and Forensic workshop with ISACA Sofia Chapter - Sofia, Bulgaria 10 Jun
• Threat Day with ISACA Sofia Chapter - Sofia, Bulgaria - 11 Jun
• South Africa Threat Day (Anomali) - Sandton, South Africa 12 Jun
• Annual FIRST Conference - Edinburgh, UK 16 Jun
• International Cybersecurity Congress by Sberbank - Moscow, Russia 20 Jun
• Softline Security Club - Moscow, Russia 26 Jun
• Interpol World 2019 - Singapore 2 July
• FS-ISAC Summit Asia - Singapore 10 July
• RSA Conference 2019 - Singapore 16 July
• CTF Summer School - Moscow region Russia 2 Aug

• 2nd Annual Indonesia Security Summit 2019 - Jakarta, Indonesia 3 Sep
• 76 AP TLD; Iskandar Puteri - Malaysia 5 Sep
• ASEAN Banking Cybersecurity Conference - Bangkok, Thailand 6 Sep
• Croc Information Security Conference - Cyprus 12 Sep
• inTech 2019 - Bishkek, Kyrgyzstan 13 Sep
• Future 2019 - Singapore 19 Sep
• Mobile Forensics Days 2019 - Moscow, Russia 19 Sep
• Europol-Interpol Cybercrime Conference - Hague, Netherlands 9 Oct
• 8th Regional Cybersecurity Summit - Muscat, Oman 28 Oct
• Countermeasure 2019 - Ottawa, Canada 7 Nov
• Threat Intelligence Benelux Summit - Amsterdam, Netherlands 12 Nov

• Automating Fraud and Financial Crime Prevention in Retail Banking - London, UK 13 Nov
• Antifraud Russia 2019 - Moscow, Russia 4 Dec
• RIW Russian Internet Week - Moscow, Russia 12 Dec
Achievement

- Annual Group-IB's CyberCrimeCon event in Singapore and Moscow
- Over 130 events for clients and partners
- Over 40 press releases and 3700 international publications
- Over 50 training events for schools and universities
- Provide trainings of several information security courses
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