CyberSecurity MALAYSIA

Corporate Profile

SECURING
OUR
CYBERSPACE

Table of Contents

Corporate Overview

CyberSecurity Malaysia is the national cybersecurity specialist agency under the purview of the Ministry of Digital.

With effect from 10 January 2024, CyberSecurity Malaysia is placed under Ministry of Digital.

CyberSecurity Malaysia is committed to provide a broad range of cybersecurity innovation-led services, programmes, and initiatives to reduce vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace.

The agency provides the following specialised cybersecurity services.

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

Vision, Mission and Strategic Theme

Vision

World-class cybersecurity specialist agency.

Mission

Leading the development of a safer and more resilient cyber ecosystem to enhance national security, economic prosperity, and social harmony through

- Provision of quality and impactful services.
- Frontier-expanding cyber knowledge and technical supremacy.
- Continuous nurturing of talent and expertise.

Strategic Theme

- Partner in Driving National Agenda.
- Quality & Impactful Service/Projects.
- Integrated Development & Delivery.
- Technical Excellence & Capacity Enhancement.
- Financial Sustainability.

History of CyberSecurity Malaysia

1997

13 January 1997

The journey started with formation of the Malaysia Computer Emergency Response Team or MyCERT (www.mycert.org.my) as a unit under MIMOS Berhad (www.mimos.my)

2001

2001

The National ICT Security and Emergency Response Centre (NISER) was established as a Department in MIMOS Berhad, and Malaysia Computer Emergency Response Team (MyCERT) was placed under NISER

2005

28 September 2005

The Cabinet decided for NISER to spun-off from MIMOS Berhad as a Company Limited-by- Guarantee under the Ministry of Science, Technology and Innovation (MOSTI)

2007

30 March 2007

NISER was officially registered as CyberSecurity Malaysia

20 August 2007

CyberSecurity Malaysia was officially launched by the Prime Minister of Malaysia

2018

19 October 2018

The Cabinet Meeting chaired by the Prime Minister of Malaysia decided CyberSecurity Malaysia to be placed under the Ministry of Communications and Multimedia Malaysia (K-KOMM)

Our journey started with formation of the Malaysia Computer Emergency Response Team or MyCERT (www.mycert.org. my) on 13 January 1997 as a unit under MIMOS Berhad (www.mimos.my). On 24 January 1998, the National Information Technology Council (NITC) chaired by the Prime Minister of Malaysia proposed for the establishment of an agency to address emerging ICT security issues in Malaysia. As a result, the National ICT Security and Emergency Response Centre (NISER) was formed in 2001 as a Department in MIMOS Berhad, and MyCERT was placed under NISER.

The Cabinet Meeting on 28 September 2005, through the Joint Cabinet Notes by the Ministry of Finance (MoF) and Ministry of Science, Technology and Innovation (MOSTI) No. H609/2005 agreed to establish NISER (now known as CyberSecurity Malaysia) as a National Body to monitor the National e-Security aspect, spun-off from MIMOS Berhad to become a separate agency and incorporated as a Company Limited-by-Guarantee. On 30 March 2007, NISER was registered as a not-for-profit, Company Limited-by-Guarantee under supervision of MOSTI.

The NITC Meeting No. 1/2006 decided to implement the National Cyber Security Policy (NCSP) led by MOSTI. NISER was mandated to provide technical support for NCSP implementation and was rebranded to CyberSecurity Malaysia to reflect its wider mandate and larger role. On 20 August 2007, the Prime Minister of Malaysia officiated CyberSecurity Malaysia and launched its new logo.

Board of Directors

General Tan Sri Dato' Sri (Dr.) Haji Zulkifeli Bin Mohd Zin (Retired)
Chairman, Board of Directors

Datuk Mohamad Fauzi bin Md Isa
Secretary General of the Ministry of Communications

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab FASc
Director / Chief Executive Officer

Shaifubahrim Bin Mohd Saleh
Director

Dato' Dr. Suhazimah Binti Dzazali
Director

Dr. Fazidah Binti Abu Bakar
Director

Management Committee Members

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab FASc
Chief Executive Officer

Roshdi Bin Hj Ahmad
Chief Operating Officer (COO)

Ts. Mohd Zabri Adil Bin Talib
Acting Chief Technology Officer (CTO)

Dr. Maslina Binti Daud
Senior Vice President,
Cyber Security Proactive Services Division

Ts. Mohd Shamir Bin Hashim
Senior Vice President,
International & Government Engagement Division

Lt. Col. Mustaffa Bin Ahmad (Retired) C/CISO psc
Senior Vice President,
Outreach and Capacity Building Division

Jailany Bin Jaafar
Head,
Legal & Secretarial/Company Secretary

Azman Bin Ismail
Vice President,
Corporate Services Division

Milestones & Achievement

National ICT Security & Emergency Response Centre (NISER)

No	Year	Milestones & Achievement
1	13 January 1997	The Malaysia Computer Emergency Response Team (MyCERT) was established under MIMOS Berhad.
2	24 January 1998	The Government of Malaysia through the National Information Technology Council (NITC) Meeting 6/98 decided to establish the National ICT Security & Emergency Response Centre (NISER) to address information security issues at national level.
3	30 October 1998	Government's Internet and IT Committee or *Jawatankuasa IT dan Internet Kerajaan* (JITIK) decided to place NISER under MIMOS Berhad. MyCERT became a part of NISER.
4	28 May 1999	The Strategic Thrust Information Committee (STIC) Meeting 1/99 expanded the function of NISER to address cybersecurity initiatives at national level by "creating, monitoring, and updating the defence and security systems against cyber threats" together with other Government agencies.
5	1 November 2000	NISER became fully operational.
6	10 April 2001	NISER was officially launched by the Deputy Prime Minister of Malaysia.
7	17 July 2001	NISER organised the 1st NISER/SANS Asia Pacific Conference (first professional certification program organised by NISER).
8	7 November 2001	NISER Panel of Experts was established.
9	29 April 2002	NISER Computer Forensic Service was launched.
10	19 August 2002	NISER co-founded APCERT (Asia Pacific Computer Emergency Response Team) and was entrusted to represent APCERT at APECTEL 26th Meeting in Moscow, Russia.
11	16 May 2003	NISER was accepted to the Forum of Incident Response and Security Teams (FIRST).
12	10 March 2003	NISER co-launched the Information Security Management Systems (ISMS) certification scheme with SIRIM. The scheme aims to provide Malaysian organisations with the opportunity to demonstrate their compliance with international standard.
13	26 February 2004	NISER led the establishment of 1st Working Group in Business Continuity Management in Malaysia.

No	Year	Milestones & Achievement
14	23 June 2005	Proposal for the collaboration of Computer Emergency Response Teams (CERTs) among the Organisation of Islamic Cooperation (OIC) member countries was adopted during the Islamic Development Bank's Board of Governors Meeting.
15	4 July 2005	NISER established a Task Force for the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT) consisted of representatives from Malaysia, Pakistan, Tunisia, UAE and Nigeria.

Transformation of NISER to CyberSecurity Malaysia

No	Year	Milestones & Achievement
1	28 September 2005	The Cabinet Meeting, through the Joint Cabinet Notes by the Ministry of Finance (MOF) and Ministry of Science, Technology and Innovation (MOSTI) No. H609/2005 agreed to spin off NISER from MIMOS Berhad.
2	14 March 2006	NISER was incorporated as a Company Limited By Guarantee (CLG), which marked the official spun off from MIMOS Berhad to become a separate agency and a National Body to monitor the National e-Security aspects, under the purview of MOSTI.
3	1 June 2006	NISER operated independently and was segregated from MIMOS Berhad.
4	17 November 2006	Relocation of NISER's operation and corporate office from MIMOS Berhad at Technology Park Malaysia to Sapura@Mines Building at The Mines Resort City.
5	30 March 2007	NISER's brand name changed to CyberSecurity Malaysia to better reflect its expanded roles, which include coordination and implementation of the National Cyber Security Policy (NCSP).
6	20 August 2007	The Prime Minister of Malaysia launched CyberSecurity Malaysia's logo and brand name, which marked the official rebranding and transformation of NISER to CyberSecurity Malaysia.

CyberSecurity Malaysia

No	Year	Milestones & Achievement
1	1 January 2006	Digital Forensics team in CyberSecurity Malaysia recognized as 'expert witness' in accordance with the Criminal Procedure Code 399 subsection 3(F).
2	8 February 2007	CyberSecurity Malaysia (first organisation in Malaysia) was appointed as the Chair of Asia Pacific Computer Emergency Response Team (APCERT) and Steering Committee Members.
3	24 July 2008	CyberSecurity Malaysia coordinated the first National Cyber Crisis Exercise (Cyber Drill) code-named X-MAYA in collaboration with the National Security Council.
4	25 July 2008	CyberSecurity Malaysia obtained full certification in Information Security Management System (ISMS), ISO/IEC 27001.
5	8 October 2008	The Government of Malaysia appointed CyberSecurity Malaysia as the sole Certification Body for evaluation and certification scheme based on MS ISO/IEC15408:2005 Information technology - Security Techniques - Evaluation Criteria for IT Security.
6	15 January 2009	CyberSecurity Malaysia elected as the Chair of Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT), making Malaysia the first country to chair the OIC-CERT.
7	7 July 2009	The Minister of Science, Technology and Innovation (MOSTI) launched CyberSecurity Malaysia's Cyber999 Help Centre.
8	8 July 2009	CyberSecurity Malaysia introduced the Malaysia Cyber Security Awards to honour organisations and individual for their contribution and commitment towards cybersecurity industry.
9	2 November 2009	The official opening of first CyberSecurity Malaysia regional office, serving Northern Region located at Perak Techno-Trade Centre in Ipoh, Perak.
10	1 December 2009	The Minister of Science, Technology and Innovation, (MOSTI) launched CyberSecurity Malaysia's Malware Research Centre at the World Computer Security Day celebration in Kuala Lumpur.
11	15 March 2010	CyberSecurity Malaysia's Security Assurance Lab obtained MS ISO/ IEC 17025:2005 accreditations which enable the lab to provide vulnerability assessment for ICT equipment and systems.
12	24 September 2010	The Deputy Prime Minister of Malaysia who was also the Minister of Education, launched 'CyberSAFE in Schools', a cybersecurity awareness programme for primary and secondary school children as well as teachers.
13	26 November 2010	The Government of Malaysia appointed CyberSecurity Malaysia as the Certifier and Evaluator of Malaysia Trustmark for the Private Sector (MTPS).
14	1 May 2011	Establishment of Information Security Management System Audit and Certification Scheme (CSM27001) in support of the National Cyber Security Policy (NCSP).

No	Year	Milestones & Achievement
15	27 September 2011	CyberSecurity Malaysia accepted by the Common Criteria Recognition Arrangement (CCRA) as Certificate Authorizing Participant, the first among ASEAN member countries to become Certificate Authorizing Member of the Common Criteria ISO/IEC 15408.
16	3 November 2011	CyberSecurity Malaysia's digital forensics laboratory accredited with ISO/ IEC17025: 2005 and the ASCLD/LAB - International 2011 by ASCLD/ LAB, the first forensics laboratory in Malaysia and the Asia Pacific region.
17	17 November 2011	CyberSecurity Malaysia won the 1st Global CyberLympics Championships 2011, an ethical hacking competition for Asia Pacific Region.
18	31 December 2012	CyberSecurity Malaysia elected as the Organisation of Islamic Cooperation – Computer Emergency Response Team's (OIC-CERT) Secretariat at the 4th Annual General Meeting (AGM) in addition to being the Chair of the OIC-CERT.
19	14 January 2013	CyberSecurity Malaysia is the first organization to hold the Chairmanship of the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT) on behalf of Malaysia, thus making Malaysia the first country to chair the OIC-CERT.
20	3 July 2013	CyberSecurity Malaysia launched the Malaysia Trustmark for Private Sector (MTPS).
21	1 September 2013	CyberSecurity Malaysia spearheaded cybersecurity area for the Member Country Partnership Strategy (MCPS), International Development Bank (IDB) under Reverse Linkage Program.
22	26 November 2014	CyberSecurity Malaysia elected as the Chairman for World Trustmark Alliance (WTA)
23	1 December 2014	CyberSecurity Malaysia appointed as Co-Chairman for the Council fof Security Cooperation in the Asia Pacific (CSCAP) Study Group.
24	18 August 2015	CyberSecurity Malaysia appointed as the Training Provider for Malaysian Technical Cooperation Programme (MTCP) under the Ministry of Foreign Affairs.
25	7 September 2015	CyberSecurity Malaysia appointed as Deputy Chair of Asia Pacific Computer Emergency Response Team (APCERT), a Steering Committee Members and also led the Malware Mitigation Working Group.
26	2016	CyberSecurity Malaysia recognized as the Top 5 Contributors to the Ministry of Science, Technology and Innovation (MOSTI) KPI 2016 with 123% achievement as well as ranked third among MOSTI's agencies.
27	14 November 2017	CyberSecurity Malaysia re-appointed as the Deputy Chair of Asia Pacific Computer Emergency Response Team (APCERT) and also Steering Committee Members.
28	24 October 2018	CyberSecurity Malaysia re-appointed as Deputy Chair of Asia Pacific Computer Emergency Response Team (APCERT) and Steering Committee Members.
29	24 May 2019	CyberSecurity Malaysia accredited by INTERPOL for developing the INTERPOL Global Guidelines for Digital Forensics Laboratories.

No	Year	Milestones & Achievement
30	27 June 2019	CyberSecurity Malaysia declared Champion at the 1st ACSC-ASEAN Capture the Flag in Australia.
31	31 July 2019	CyberSecurity Malaysia Cryptographic Evaluation Lab (MyCEL) accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform cryptographic module validation and testing based on FIPS 140-2 Security Requirements for Cryptographic Modules standard.
32	1 October 2019	CyberSecurity Malaysia elected as the Chair of Asia Pacific Computer Emergency Response Team (APCERT) and Steering Committee Members.
33	1 October 2020	CyberSecurity Malaysia has been reappointed as the Chair of the Asia Pacific Computer Emergency Response Team (APCERT). for rhe duration of 2020 - 2021.
34	23 March 2021	CyberSecurity Malaysia launched SiberKASA, is an initiative to develop, empower, sustain and strengthen cyber security infrastructure and ecosystem in Malaysia to combat the growing complex and sophisticated cyber threats and cyber attacks.
35	29 September 2021	CyberSecurity Malaysia has been re-elected as a Steering Committee member (2021-2023) and the Chair of the Asia Pacific Computer Emergency Response Team (APCERT) for 2021 - 2022.

Awards

No	Year	Award
1	2008	CyberSecurity Malaysia awarded "Best Branding for Internet Security" 2008 by the Brandlaurette Malaysia.
2	2009	CyberSecurity Malaysia awarded "Best Branding for SMEs Chapter Awards" 2009 on cybersecurity by the Brandlaurette Malaysia.
3	13 October 2012	CyberSecurity Malaysia's CyberSAFE portal (www.cybersafe.my) awarded the Saramad Golden Award 2012 for "The Best Initiative in Child Online Protection" at the 6th International Digital Media Fair & Festival 2012 (IDMF 2012) in Tehran, Iran.
4	18 October 2015	CyberSecurity Malaysia conferred FireEye Award 2015 for "Best Cyber Security Innovation"
5	6 May 2016	CyberSecurity Malaysia conferred WSIS Prizes 2016 Champion for "Securing the Cyberspace through International Collaboration of the Computer Emergency Response Teams" at the World Summit of the Information Society (WSIS) 2016.
6	9 December 2016	CyberSecurity Malaysia conferred BSI Award 2016 by BSI Services Malaysia Sdn Bhd for "Training Support Excellence Award".
7	16 June 2017	CyberSecurity Malaysia conferred WSIS Prize 2017 Champion for "Collaborative Information Sharing Model for Malware Threats Analysis: A Case Study for the Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT)" at the World Summit of the Information Society (WSIS) 2017.
8	2017	CyberSecurity Malaysia received NBOS Award by the Chief Secretary to the Government of Malaysia on various projects such as Cyber999 Coordination Service, Cyber RANGE Lab Malaysia - Next Gen Cyber Defender, Evaluation and Certification of ICT Products and Digital Forensics Reference Services.
9	5 - 6 June 2018	Chairman Board of Directors, CyberSecurity Malaysia conferred Professional Award for Development of Professional Relations in Information Security by the Russian Government.
10	7 September 2020	CyberSecurity Malaysia through Global ACE Certification has been selected as one of the Champion Projects under Category 5: Building Confidence and Security in the Use of ICT at the World Summit on the Information Society (WSIS) Prize Award 2020.
11	23 March 2021	CyberSAFE^{TM} L.I.V.E. Galeri was recognised by The Malaysia Book of Records as "The First Cyber Security Gallery in Malaysia". Galeri as a hub for research, training, and to disseminate cyber security knowledge in Malaysia as part of CyberSAFE Programme.

Partnership

No	Organisation	Area of Collaboration	Year
1	Universiti Teknikal Malaysia Melaka	Development of a framework for cooperation in the area of cybersecurity research and education.	2019
2	Gujarat Forensic Science University	Development of a framework for cooperation in the area of cybersecurity research and education.	2019
3	InterExchange Solutions Limited	Exchange of information and strategies for effective cybersecurity incident response.	2019
4	RAM Credit Agency (RAMCI)	Cyber identity theft campaign initiatives.	2019
5	Digital Perak Corporation Holdings	CyberSecurity Malaysia is the preferred cybersecurity partner for Perak State Government and agencies under the State Government.	2019
6	Cyber Rescue Ltd	Collaboration in cybersecurity awareness and risk assessment guidelines for big corporations.	2019
7	Datasonic Innovation Sdn Bhd	Collaboration on Digital Identity.	2019
8	National Defence University of Malaysia, Mimos Berhad and System Consultancy Services Sdn Bhd	Cryptography development.	2019
9	Kedah Industrial Skills and Management Development Centre (KISMEC)	Cybersecurity training and services.	2019
10	Politeknik Mersing	Cybersecurity training and services.	2019
11	Universiti Tenaga Nasional (Malaysia)	Cybersecurity training and services.	2019
12	Universiti Teknologi Petronas	Cybersecurity training and services.	2019

No	Organisation	Area of Collaboration	Year
13	Universiti Teknologi Mara	Cybersecurity research and Institutional exchange of staff and students.	2019
14	Universiti Malaysia Terengganu (UMT)	Cybersecurity in Cloud Computing, Industry 4.0 and Global ACE Scheme.	2019
15	BAE Systems Applied Intelligence Limited	Collaboration on knowledge sharing, research, and development of activities to enhance the capability and capacity of cyber defence in Malaysia.	2018
16	The Statistical, Economic and Social Research and Training Centre for Islamic Countries (SESRIC)	Development and implementation of a training programme that introduce the Global ACE Scheme to the OIC Countries. Development of Global ACE Scheme country chapter.	2018
17	Alibaba Security Response Center, Alibaba (China) Co., Ltd., People's Republic of China	Exchange of information on current cyber threats in order to increase the effectiveness on cyber security incident response.	2018
18	National Information Security Forum "Infoforum"	Cooperation and develop business and professional contacts between experts and organizations of Malaysia and Russia in the field of information security.	2018
19	Cybersecurity Philippines Computer Emergency Response Team Org. Inc.	Enhance cooperation in Computer Emergency Response Team (CERT) and best practices for ICT sector.	2018
20	National Center for Cybersecurity Technology (Taiwan)	Exchange of information and sharing of knowledge on current cyber threats to increase the effectiveness of cyber security incident response as well as cross boarders incidents.	2018
21	Qatar University, State of Qatar	Explore opportunities to potentially collaborate in the relevant areas of cybersecurity.	2018
22	American Bureau of Shipping (ABS)	Cybersecurity in Maritime Industry.	2018
23	Malaysia Board of Technologies (MBOT)	Cooperation, exchanging and sharing related information in the development of related technology field which recognized by MBOT. CSM has been appointed as Technology Expert Panel (TEP).	2018
24	Bank Islam Malaysia Berhad	Cybersecurity Initiatives.	2018
25	Iskandar Regional Development Authority (IRDA)	Cybersecurity Initiatives.	2018
26	S5 Systems Sdn Bhd	Cybersecurity Initiatives.	2018
27	May Siber Teknologi	Strategic technology collaboration in cybersecurity.	2017

No	Organisation	Area of Collaboration	Year
28	Thales Communications & Security SAS	Cooperation and collaboration in the development, capabilities and capacity in information security.	2017
29	R&D Center Kazakhstan Engineering	Cybersecurity Initiatives.	2017
30	Universiti Kebangsaan Malaysia	Cooperation and development in academic and reseach.	2017
31	National Defense University of Malaysia	Cybersecurity research, knowledge sharing and joint programs.	2017
32	Perbadanan Putrajaya	Vulnerability Assessment and Penetration Testing for Smart City in Putrajaya.	2017
33	UKM Medical Centre (UKMMC)	Vulnerability Assessment and Penetration Testing on Intensive Care Unit (ICU) & Operation Theatre (OT) Medical Devices.	2017
34	Malaysia Crime Prevention Foundation (MCPF)	Cyber crime prevention and cybersecurity awareness through public engagement and strategic research.	2017
35	Malaysia Airport Holdings Berhad (MAHB)	Cybersecurity Initiatives.	2017
36	Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)	Cybersecurity Initiatives.	2017
37	Chief Government Security Office (CGSO)	Cybersecurity Initiatives.	2017
38	Korea Internet & Security Agency of the Republic of Korea (KISA)	Exchange, develop and consolidate their knowledge and experiences in the areas of: • Cybersecurity incidents and the response management. • Cybersecurity threats and risk management. • Cybersecurity training and awareness. • Cybersecurity research and development. • Critical information infrastructure protection.	2016
39	Academy of Informational Systems, Russia	Cooperate in promoting closer collaboration, interaction and exchange of information regarding national security.	2016
40	Malaysian Software Testing Board	Areas of testing, competency and infrastructure.	2016
41	Angkatan Koperasi Kebangsaan Malaysia Berhad (Angkasa)	Establishment of general framework and cooperation on cybersecurity field.	2016

No	Organisation	Area of Collaboration	Year
42	Malaysia Communication and Multimedia Commission (MCMC)	Cooperation on cybersecurity field.	2015
43	CERT Australia	Exchange if information on cybersecurity. Establishment of channels for exchange of information. Exchange of delegations and visits.	2014
44	King Saud University Kingdom of Saudi Arabia	Develop a focused cooperation in the field of cybersecurity.	2011
45	Traffic Observation and Management Limited, United Kingdom	Cooperation in information security related activities: • Research and projects. • Training programs and courses. • Professional development training.	2010
46	National Agency for Computer Security (NACS), Republic of Tunisia	Exchange of information an collaboration in the following areas of information security: training & education, incident handling, products certification, bets practices and policies, digital forensics, cryptographic technology, surveys and research.	2008

Services

Services

1. Malaysia Computer Emergency Response Team (MyCERT)

www.mycert.org.my

1.1 Cyber999 Cyber Incident Reference Center

Cyber999 Cyber Incident Reference Center provides expert service to internet users and organizations on cyber security incidents. Cyber security incidents can be reported via online form, email, phone call and Cyber999 Mobile App. Cyber999 Cyber Incident Reference Center also produces Malaysia Threat Landscape report, technical findings and analysis based on the incidents reported by Internet users.

www.mycert.org.my/cyber999

1.2 Lebahnet (Honeynet Project)

Lebahnet is based on Honeypot technology. It provides supporting information on network trends and malicious activities for MyCERT to handle incident as well as advisory activities. Honeypots is a collection of computer software mechanisms established to mimic a legitimate site to ensnare malicious software into believing that the device is in a weak position for attacks. It allows researchers to detect, monitor and counter-attack malicious activities by understanding activities completed during intrusion phase and attacks' payload.

1.3 Cyber Health Assessment (Network Compromise Assessment)

Cyber Health Assessment (CHA) was conducted using CMERP Insight (INSIGHT). INSIGHT is a Breach Detection System (BDS) to detect malicious and suspicious activities of malware inside a network after a breach occurred. It is a solution designed to identify signs of threats and alert the organization on potentially dangerous activity. INSIGHT is deployed using method out of band system which scan data mirrored from network switch activities. Advanced Persistent Threats (APT) employ various exploits on a target, depending on the type of vulnerable Internet applications used over the network.

INSIGHT assist IT personnel to detects unknown, advanced and adaptive threats. Computer Security Incident Response Team or CSIRT Consultancy provide specialized service for organizations comprising People, Process and Technology. It creates an implementation plan to develop and apply CSIRT in organizations. The consultancy also provide Incident Handling and Network Security trainings, Job Attachments, including Professional Memberships to FIRST, APCERT and OIC-CERT.

1.4 Managed Security Services

Advanced Security Operation Center (ASOC) monitor, track and response to security incidents such as Malware attacks, Intrusions, DDoS to protect organization's data and IT infrastructures especially Small Medium Enterprise (SME's) using the technology developed by local experts, Coordinated Malware Eradication & Remediation Platform Technology (CMERP).

CMERP
Detection | Eradication | Remediation

1.5 CSIRT Consultancy

Computer Security Incident Response Team or CSIRT Consultancy provide specialized service for organizations comprising People, Process and Technology. It creates an implementation plan to develop and apply CSIRT in organizations. The consultancy also provide Incident Handling and Network Security trainings, Job Attachments, including Professional Memberships to FIRST, APCERT and OIC-CERT.

1.6 Phishing Exercise (Social Engineering)

Phishing assessment assess awareness among staff within an organization by sending malicious emails. It aims is to analyse staff's responsiveness towards phishing attempt and directly measure staff compliance against internal policies and procedures.

1.7 Cyber Drill Exercise

CyberDrill is an activity conducted by MyCERT to assess organization's cyber capacity by measuring its ability to detect and respond to a security incident. This project utilize various tools and infrastructure in CSM to perform simulated cyber drill exercise that aim to identify organisations' readiness based on existing cyber security incident response procedures.

1.8 Host Malware Scanning (Host Compromise Assessment)

Host Compromise Assessment is a service to identify evidence of malicious activity within the IT assets, through analysed data retrieved from internal scanning and 3rd-party tools. This assessment includes several stages, planning, preparation, execute, identify and reporting, to identify malware activities.

2. Digital Forensics

2.1 CyberDiscovery

CyberDiscovery

- **Digital Forensics (DF) Case Management (CyberDiscovery)**
- **Incident Handling Case Management (CyberDiscovery)**

CyberDiscovery is a professional cyber forensics service for public, individual or private organization. It addresses concerns on Electronic Stored Information (ESI) as digital evidence, in order to provide answers for questions raised in a civil litigation. It provides the following services:

- Onsite Evidence Preservation
- Evidence Analysis
- Expert Witness in Court

2.2 X-Forensics Tools

X-Forensik: Evidence Preservation Tools is a series of digital forensic tools developed for digital data preservation ensuring its integrity and admissibility as evidence in judicial proceeding.

2.3 PenDua Tool

PenDua
x-Forensik 2.0

Pendua is a forensically sound portable digital file duplicator. It is used to duplicate digital document from a computer and its hashing function complies to forensics and evidence admissibility requirements. It also provides activity log critical in an investigation. Pendua tool is developed under X-Forensik initiative.

2.4 Kloner

Kloner
x-Forensik 2.0

Kloner is a forensically sound data acquisition tool embedded with Cloning, Imaging and Wiping capabilities. Its write-protect and hashing functions comply to forensics and evidence admissibility requirements. Kloner assist investigators to preserve digital evidence at crime scene. Kloner tool is developed under X-Forensik initiative.

2.5 DataHapus

DataHapus
x-Forensik

x-Forensic DataHapus is a high-powered and user-friendly data sanitization device with a GUI touch display. x-Forensic Data Sanitization sanitize hard disk thoroughly to ensure all confidential files are permanently deleted before disposal. DataHapus tool is developed under X-Forensik initiative.

2.6 CamMuka

CamMuka 2.0

CamMuka is a forensically sound facial recognition system to perform facial recognition of the unknown face with the known face. It is utilized in investigation of criminal cases, where the result of the recognition analysis is accepted by the court.

The Artificial Intelligence (AI) behind CamMuka is proven and backed up by scientific journals. CamMuka system applications are supported with SOPs and methodologies comply with digital forensic international standards.

2.7 Digital Forensics Quality Management System Expert Consultation

Digital Forensics Quality Management System Expert Consultation service assist digital forensics lab to develop digital forensics policy and procedures based on international standard ISO 17025 requirements. It enable organisations to develop competent staff, provide controlled environment and equipments, to produce high quality digital forensics results, admissible in court of law and fulfill customers expectation.

We are committed to provide quality and accurate forensics outcome in line with international requirement ISO 17025. We are proud to tell you that we have been accredited with ANSI National Accreditation Body (ANAB) since 2011.

Categories Of Digital Forensics

Media and file system forensics
Examines data in all digital storage media including hard drives, USB flash drive, flash memory card, compact disc and many more.

Operating system forensics
Examines operating systems including Windows, Mac OS or Linux.

Web and email forensics
Examines web cookies, browser history, and other items that can help locate and identify email account administrator.
Social network forensics
Examines pertinent social media data of a social media profile.

Database and malware forensics
Examines the collection and access of data within pertinent databases and malicious codes or software.

Network forensics
Examines network traffic data and cyber-attacks such as intrusions within computer or digital networks.

Mobile device forensics
Examines different types of data collected in mobile devices including smartphones, tablet computer or IoT devices.

Multimedia forensics
Examines the authenticity and content analysis of multimedia file, including identification of a person or an object.

Software forensics
Examines software or source codes author information behind a specific software.

Cloud forensics
Probes and examines cyber-attacks and other pertinent data within cloud systems.

Virtual systems forensics
Examines and valuates the data and collection of virtual machines.

3. Cryptography Development

mykripto.cybersecurity.my

Cryptography Development (CD) was established in 2007 to spearhead the research and development in various areas of cryptography. Through MyCEL lab (accredited by National Voluntary Laboratory Accreditation Program (NVLAP), USA), CD is now able to perform evaluation on the correct implementation of cryptography through module and algorithm validation services. CD continuously engages with the cryptography experts in Malaysia to support activities in one of the National Cryptography Policy's Strategic Approach.

Our goal is to increase organisational's data protection, confidentiality and integrity through the use of evaluated and certified cryptographic modules and algorithms

CDD Objectives:

- To increase trust on the use of cryptography technology in IT products and digital environment; and
- To provide expertise in cryptographic modules and algorithms validation in compliance with FIPS 140 standard and ISO/IEC 19790 standard

3.1 MyKripto Validation

MyKripto Validation is a security validation and analysis service that include the following:

- Cryptanalysis of a cryptographic algorithm to gauge its security strength
- Cryptographic algorithm conformance testing against a standard document
- Determine randomness characteristics of a random generator

3.2 CyberSecurity Malaysia Cryptographic Evaluation Lab (MyCEL)

CyberSecurity Malaysia Cryptographic Evaluation Laboratory (MyCEL) was accredited by the National Voluntary Laboratory Accreditation Program (NVLAP), USA.

NVLAP®
TESTING
NVLAP LAB CODE 600138-0

With this accreditation, MyCEL is able to conduct evaluation and validation activities of cryptographic modules contained in a security product based on FIPS140 security requirements. This enhance user's security and develop trust in using cryptographic module in security products.

Apart from FIPS140, MyCEL also conduct cryptographic module validation based on ISO/ IEC19790 requirements and cryptographic algorithm validation based on MySEAL

3.3 Blockchain Security Assessment

Blockchain Security Assessment is a service to validate and verify security properties in a blockchain and smart contract. Businesses gain insight on its overall blockchain and smart contract security posture, and improve the ability to address potential flaws in their blockchain based solutions or applications.

CSM MySEF
Malaysian Security Evaluation Facility

4. Malaysian Security Evaluation Facility (MySEF)

MySEF is a licensed evaluation facility under Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme. It aims to create a safe and reliable computing environment through the provision of ICT security evaluation.

mysef.cybersecurity.my

MySEF provides expertise in ICT Security Evaluation and Testing Services as follow:

4.1 ICT Product Security Assessment (IPSA)

IPSA is a security functional testing and/or vulnerability assessment and penetration testing adapting ISO/IEC 15408 Common Criteria (CC) and ISO/IEC 18045 Common Methodology for Information Technology Security Evaluation (CEM) referring (but not limited to) Malaysian Standards (MS) and best practices.

4.2 Common Criteria Laboratory Development and Advisory Services

Based on our experience providing Common Criteria Evaluation to our clients, we provide technical services & advisory to existing and potential CC laboratories. It mainly consists of Standard Operating Procedure (SOP) development, accreditations preparations, laboratory facilities check and audit session/s. Our technical expert will offer in-depth industry experience in many areas including up-to-date information and regulatory on Common Criteria service.

4.3 ISO 17025 Professional Laboratory Service and Specialized Equipment

ISO/IEC 17025 Professional Laboratory Service is offered to external laboratories for laboratory/equipment rental and Inter-Laboratory Comparison (ILC) exercise.

- Laboratory/equipment rental for ICT products testing and evaluation services;
- Inter-Laboratory Comparison (ILC) exercise is mandatory for any ISO/IEC 17025 Test Lab in

Malaysia. CSM MySEF offer this service based on the Scope of Work (SOW) agreed by both Test Labs including security evaluations, security functional testing or penetration testing.

4.4 Cloud Security Services (Cloud Security Readiness Assessment)

The scope of Cloud Security Readiness Assessment requirements focus on cloud security audit on IaaS, PaaS and SaaS platform for Cloud Service Subscribers (CSS), Cloud Service Providers (CSP) and Cloud Service Brokers.

Cloud Security Readiness Assessment may be conducted independently for none ISMS complying Cloud Service Subscribers (CSS), Cloud Service Providers and Cloud Service Brokers.

The scope of Cloud Security Readiness Assessment for ISMS requirements focus on cloud security audit on IaaS, PaaS and SaaS platform for Cloud Service Subscribers (CSS), Cloud Service Providers (CSP) and Cloud Service Brokers.

Cloud Security Readiness Assessment for ISMS can be conducted as an extension on Cloud scope on top of Information Security Management System (ISMS) Certification.

4.5 Cloud Security Services (Cloud Security Vulnerability Assessment)

The scope of Cloud Security Vulnerability Assessment involve Vulnerability Assessment & Penetration Testing on Cloud SaaS and/or PaaS for Cloud Service Provider (CSP).

- Vulnerability Assessment (VA) is performed by assessors in determining common threats, loopholes and weakness of cloud solution deployed in the forms of PaaS and/or SaaS.
- Penetration Testing is an activity to exploit weaknesses of the cloud solution deployed in the form of PaaS and/or SaaS.

5. Malaysia Vulnerabilities Assessment Centre (MyVAC)

Malaysia Vulnerability Assessment Centre or MyVAC is a department within CyberSecurity Malaysia. The centre is formed to enhance the national information security ecosystem and increase nation's ability in defending against cyber threats and exploitation due to information systems and technology vulnerabilities.

MyVAC recognizes the importance of having vulnerability assessment laboratories for critical information systems and technologies. In the laboratory (test bed), MyVAC analysts conduct assessments, identify common and potential vulnerabilities and investigate mitigation approaches.

Strategic Objectives
The strategic objectives are:

- To develop a comprehensive cyber security programme as a national priority that provides mitigation strategies to prevent the exploitation of critical information systems and technology vulnerabilities.
- To reduce vulnerabilities and security risks by providing vulnerability assessment and countermeasures.
- To develop the cyber security capacity and capability required primarily to ensure that the information systems and technologies could be used safely or implemented securely within the Critical National Information Infrastructure (CNII).
- To promote the awareness and educate CNII owners and stakeholders about the vulnerabilities and possible attacks to their critical infrastructures.
- To build partnerships among critical industries, CNII owners and stakeholders, governments and researchers to plan, develop and share security solutions.

5.1 Security Posture Assessment (SPA)

- Security Posture Assessment is an exercise to identify security loopholes in an organization
- Include service process diagram (if possible/ necessary)
- Method and approach based on international standard OWASP, OSSTMM, and PCI-DSS
- Effective security risk assessment to prevent breaches, reduce impact of realized breaches, and protect company's reputation

5.2 Vulnerability Assessment & Penetration Testing (VAPT)

Vulnerability Assessment and Penetration Testing (VAPT) is a service offered to public and private organizations to discover and highlight security issues at client environment. It provides recommendations and countermeasures to rectify vulnerabilities in order to reduce risk of security breach.

6. CyberSecurity Industry Engagement and Collaboration (CIEC)

Among the services offered by CyberSecurity Industry Engagement and Collaboration are the CyberSecurity Malaysia Collaboration Program (CCP); Cybersecurity Malaysia Awards, Conference and Exhibition (CSM-ACE) and My CyberSecurity Clinic (MyCSC).

6.1 CyberSecurity Malaysia Collaboration Program (CCP)

CyberSecurity Malaysia Collaboration Program (CCP) serve as a strategic collaboration initiative with local cyber security industry as well as other government entities to encourage development and innovation of Malaysia's cyber security products and services. CCP provide access to potential collaborations and synergies with CyberSecurity Malaysia, related government entities and with other collaborators. This leverages partners' strengths and bridge market gaps by providing high quality and highly relevant cyber security products and services.

ccp.cybersecurity.my

6.2 CyberSecurity Malaysia Award, Conference and Exhibition (CSM-ACE)

Cyber Security Malaysia - Awards, Conference & Exhibition (CSM-ACE) is a public-private partnership driven platform for knowledge sharing and cybersecurity professional development. It serves as a forum for cybersecurity experts to discourse on cybersecurity current issues, trends, technology and innovations and to recognize contribution of individuals and organizations in the field of cyber security. CSM-ACE overview the following:

- To act as a catalyst in driving innovation and growth for the cyber security industry.
- To inculcate cyber security culture and awareness at national level.
- To gather industry experts and communities on the latest cyber security trends.
- To provide a platform for industry discourse on Malaysia's cybersecurity development and innovation towards national economic growth.
- To create greater awareness and educate small and medium-sized enterprises (SME) to nurture a culture of protecting against cyber threats

www.csm-ace.my

6.3 MyCyberSecurity Clinic (MyCSC) - Data Recovery and Data Sanitization Services

MyCyberSecurity Clinic provide trustworthy and convenient data recovery and data sanitization services that handle data in a safe, secured and confidential manner.

- Data Recovery Service - a solution to recover data from damaged, failed, corrupted or inaccessible digital storage media.
- Data Sanitization Services - address the organization's need for safe and secure deletion of data from storage devices that are retired, upgraded or reallocated.

www.cybersecurityclinic.my

7. Information Security Certification Body (ISCB)

Expanding and demonstrating professional expertise from encounters with new experiences and an endlessly changing horizon.

Information Security Certification Body or ISCB is a department within CyberSecurity Malaysia that manages certification services focusing on the information security. ISCB provides certification services against international standards and guidelines.

iscb.cybersecurity.my

7.1 Information Security Management System (ISMS) Certification

CyberSecurity MALAYSIA
ISO/IEC 27001

CyberSecurity Malaysia Information Security Management System (ISMS) Audit and Certification (CSM27001) Scheme is an audit and certification services offered to the organizations based on ISO/IEC 27001 standard. It identifies data security breaches and reduces information security risks in an organization. Effective ISMS ensure organizational confidentiality, integrity and availability of information, thus, achieve business efficiency and minimise business loss.

7.2 MyTrustSEAL

MyTrustSEAL
Certified.Recognised.Assured

MyTrustSEAL is a web seal issued to company's website after it fulfils MyTrustSEAL principles based on the scope being identified:

- Secured website and online transaction
- Compliance to Malaysian Communications & Multimedia Content Code
- Compliance to personal data protection - PDPA 2010

7.3 Penetration Test Service Provider (PTSP) Certification

ISCB
Information Security Certification Body
PENETRATION TEST SERVICE PROVIDER (PTSP)

Certification Penetration Test Service Provider (PTSP) is a national scheme provided to local penetration testing service providers and organizations that require penetrating test services. The service encourages

local cybersecurity industries' development and competitiveness to ensure organizational ethics are practiced according to guideline and best practices.

7.4 Behavioural Competency Assessment (BCA)

A psychometric test designed to measure behavioural competency that contributes to professional excellence in information security roles, providing a scientific method and performance feedback in a structured consistent and systematic way.

7.5 Privacy Information Management System (PIMS) Certification

The ISO/IEC 27701 standard assists organisations to establish, maintain & improve a Privacy Information Management System (PIMS) by enhancing an ISMS based on the requirements of ISO/IEC 27001 and guidance of ISO/IEC 27002.

7.6 Technology Security Assurance (TSA)

Technology Security Assurance (TSA) is a national scheme developed for product evaluation and certification. It is MyCC fast-track which include security evaluation, certification and assurance maintenance. The Security Functionality Testing and Penetration Testing evaluate local ICT products to identify vulnerability and assist organizations to understand and improve its security features.

7.7 Malaysian Common Criteria Scheme (MyCC) Certification

Malaysian Common Criteria Evaluation and Certification (MyCC) is an ICT products or Protection Profile (PP) security evaluation based on Common Criteria (CC), an international standard based on ISO/IEC 15408 Common Criteria (CC) and ISO/IEC 18045 Common Evaluation Methodology. Information Communication and Technology (ICT) products or/and Protection Profile (PP) are evaluated against CC requirements to determine its security fulfil certain assurance level.

7.8 Business Continuity Management System (BCMS) Certification

CyberSecurity MALAYSIA
ISO 22301

Certification BCMS Certification Scheme is a service offered to various organizations which envision resiliency based on ISO 22301 international standard. It helps to plan an effective business continuity management to protect, reduce and ensure business recovers from disruptive incidents.

7.9 Malaysian Cryptography Validation Scheme (MyCV) Certification

ISCB
Information Security Certification Body
MALAYSIAN CRYPTOGRAPHY VALIDATION (MyCV)

Malaysian Cryptography Validation (MyCV) Scheme categorised under Product Certification in ISCB services. MyCV Scheme is developed to provide the Cryprographic Module Validation (CMV) and the Cryptographic Algorithm Validation (CAV) services.

MyCV is a national scheme to provide the Cryptographic Module Validation (CMV) and the Cryptographic Algorithm Validation (CAV) services that supports Dasar Kriptografi Negara (NCP) implementation.

8. Outreach & Corporate Communications (OCC)

8.1 CyberSAFE

CyberSAFE
Cyber Security Awareness For Everyone

Let's Make The Internet A Safer Place
Through our Outreach program, we aim to inculcate cybersecurity awareness and help foster a safer digital world. In helping users protect their devices and information online, we emphasise a culture of digital citizenship among the masses from all occupations and lifestyles.

www.cybersafe.my

8.2 CyberSAFE^{TM} L.I.V.E Galeri

CyberSAFE
LIVEGALERI

CyberSAFE^{TM} L.I.V.E. Galeri was built as one of the initiatives under CyberSAFE^{TM} Program aims to foster awareness and disseminate information on cyber security and safety as well as to increase understanding and interest in the cyber security field. The concept is to display and showcase hands-on product and information besides futuristic view on our daily routine involving Internet of Things, data as well as information exchange and gathering in today's cyber world.

These information are expected to raise public awareness on the importance of cyber security including CyberSecurity Malaysia roles and functions. Students are exposed on critical subjects in cyber security field such as Science, Technology, Engineering and Mathematics (STEMS), for instance, description on Mathematics algorithm role in Cryptography.

CyberSAFE^{TM} L.I.V.E Galeri has been recognised by the Malaysia Book of Records as the 'First Cyber Security Gallery' in Malaysia. It is a hub for learning and teaching as well as disseminating information on cyber security.

L.I.V.E stands for Learning, Interactive, Virtual & Experiential

- Learning - Inductive learning environment
- Interactive - The modules and activities provided are interactive
- Virtual - Realizing the virtual world to the physical world and vice versa
- Experiential - At the end of the visit, visitors gain new experience and learn cybersecurity knowledge, advancement and guidelines

9. Cyber Security Professional Development

Driving the nation's cyber security capacity-building landscape to empower the competitive nature of cyber security practitioners and professionals (motto)

In a bid to create a knowledgeable and capable generation; able to understand and handling the ever-evolving cybersecurity threats, CSPD strives to nurture the cyber security workforce with the required knowledge, skills and attitude by providing cyber security competency courses and professional certification program which is internationally recognised.

This is effectively accomplished by infusing cyber security expertise throughout Malaysia and strengthening further through strategic collaborations with international organisations. As a body entrusted to ensure the security of Malaysia's cyberspace, our capacity building expertise is widely sought-after in the domain of:

- Digital Forensics
- Incident Handling and Response
- Security Assurance
- Cryptography
- Cyber Security Management

The list of programmes offered by CyberSecurity Malaysia includes but not limited to:

Competency Trainings:

- Security Essential
- Business Continuity Management
- Cryptography
- Common Criteria
- Digital Forensics Essential
- ISO/IEC 27001
- Network Security Assessment
- Web Application Security Assessment
- Server & Desktop Security Assessment

Certified Program under Global ACE Certification:

- Certified Digital Forensic for First Responder (CDFFR)
- Certified Information Security Management System: Internal Auditor (CISMSA)
- Certified Penetration Tester (CPT)
- Certified Secure Application Practitioner (CSAP)
- Certified Information Security Awareness Manager (CISAM)
- Certified Data Security Analyst (CDSA)
- Certified Cybersecurity Awareness Educator (CCAsE)
- Certified Security Operation Centre Analyst (CSOC)

- Certified Incident Handling and Network Security Analyst (CIHNSA)
- Certified MyCC Evaluator (CME)
- Certified Secure Web Application Developer (CSWAD)
- Certified Industrial Control System Security Analyst (CICSSA)
- Certified IoT Security Analyst (CISA)
- Certified Mobile Application Security Analyst
- Certified Cybersecurity Data Science Analyst

10.CyberGURU

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberGURU is a platform to nurture cyber security practitioners and professionals through various competency training courses and certification programs. It promotes knowledge sharing and transfer of knowledge with leading industry experts, as well as academicians and policy makers. CyberGURU has more than 20 years' experience in providing cyber security capacity building programs in Malaysia. CyberGURU delivers diverse lineup of competency courses and professional certification programs aimed at meeting the accelerating needs of today's ever-changing cyber landscape; from fundamental to certification tracks, in the domain of Incident Handling and Response, Digital Forensics, Security Assurance, Cryptography and Cyber Security Management.

www.cyberguru.my

10.1 Global Accredited Cybersecurity Education (ACE) Scheme

GLOBAL ACE
CERTIFICATION

Global ACE Certification 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 cyber security domains and the requirements of professional memberships.

This professional certification scheme is a large-scale systematic plan of actions to certify and recognise the cybersecurity workforce. It is an industry driven and vendor-neutral, developed in collaboration with government agencies, industry partners and academia.

The establishment of the scheme is in tandem with international standards such as ISO 9001 on processes, ISO/IEC 17024 on certification of persons and ISO/IEC 27001 on security management, which is vital to:

- Assure workforce capability and experience;
- Secure and validate core skills, knowledge, attitude and experience; and
- Assure trustworthiness, ethical conduct, and responsibility

The Global ACE Certification aims to enhance the skill-sets of the cybersecurity workforce congruent with local and international requirements. Global ACE Scheme Recognition Arrangement permits mutual recognition of certified cybersecurity workforce across the country boundaries. It creates value for the cybersecurity industry and elevates the security-facet of participating countries.

www.globalace.org

11. Information Security Management & Assurance (ISMA)

Established in 2006, its' primary role to drive information security management and business continuity management for CyberSecurity Malaysia. Since 2010 the department has gradually evolved to provide advisories, guidance and training for public and private sectors locally and internationally. In 2015 the department has changed the name to Information Security Management and Assurance to reflect the expansion of services covering information security governance and privacy protection.

Our Goal:
Increase organizational assurance level in the areas of cyber security governance, risk management, compliance and privacy protection and improve organizational resilience.

Objectives:

- To provide expertise for the organizations to operate in a proper conduct in accordance with risk appetite, conformance with privacy and information security requirements;
- To assist organizations in improving their preparedness and ensuring the continuity of their services.

Among the services offered by ISMAD are:

11.1 Information Security Governance, Risk & Compliance Health Check Assessment (ISGRiC)

ISGRiC
Information Security Governance, Risk & Compliance
ASSESS . ANALYSE . ADVOCATE

A service to assist organisations to determine current level of readiness and initiatives in information security governance, risk management and compliance thus, ensure management make informed decisions based on ISGRiC results, justify the information security investment and support business case for managing information security.

isgrc.cybersecurity.my

11.2 Information Security Management System (ISMS) Guidance Series

A service that provides expert guidance to organisations for the protection and preservation of confidentiality, integrity and availability of information and information systems through implementation of information security management in accordance to ISO/IEC 27001 Information Security Management System (ISMS) requirements.

11.3 Privacy Information Assessment

A service to conduct compliance and impact assessment on organisations that collect, store and process personal identifiable information (PII) covering technology, process and people. This is to ensure data privacy protection is uphold in accordance to relevant acts and international standards (Malaysia PDPA Act709 and ISO/IEC 27701).

- Data Privacy Jurisdiction Risk Assessment (PJuRA)
- Data Privacy Impact Assessment (DPIA) (*development is in progress, to be completed in 2022)

12. Government & International Engagement

Our strategic engagement with the Malaysian Government is aimed at identifying and driving various government collaborations, working relations and activities to advocate the cyber security agenda.

Other than engaging local stakeholders, we also have a International Strategic Engagement Programme to facilitate cross-border cooperation.

CyberSecurity Malaysia is the co-founder of the Asia Pacific Computer Emergency Response Team (APCERT) and Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT). Since the formation of these two collaborative platforms, CyberSecurity Malaysia has been playing a very active roles as Steering Committee member. In recognition of these efforts, CyberSecurity Malaysia has been appointed as the Chair and upon reaching end of the term, CyberSecurity Malaysia was elected as the Permanent Secretariat of the OIC-CERT. In APCERT, CyberSecurity Malaysia has been appointed as the Deputy Chair.

12.1 Government Engagement (GE)

Government Engagement offers strategic engagement services with stakeholders within the Malaysian Government. It aims to identify and lead various national cybersecurity initiatives, programmes, collaborations, and activities to advocate and enhance the prominence of cybersecurity agenda for the nation. This service also provides administration for the Critical Information Infrastructure Protection (CIIP) portal

ciip.cybersecurity.my

12.2 International Engagement (IE)

International Engagement provides multilateral relations service to enhance cyber security corporation globally among the Computer Emergency Response Teams (CERTs) and other information security organizations. It assists CyberSecurity Malaysia to establish and support cross border collaboration, bilateral and multilateral platforms in the effort to achieve a safe and secured cyber space.

www.oic-cert.org

13. Strategic Study & Research

Sharpening the instrument of transformation by bringing together cutting-edge community engaged research in a continuously evolving landscape.

The Strategic Research Division of CyberSecurity Malaysia is responsible for developing, coordinating and stimulating a continuous research activity at CyberSecurity Malaysia within the cyber security domain.

CyberSecurity Malaysia's Strategic Research Division is responsible to plan, execute and accomplish strategic research directions and framework of CyberSecurity Malaysia. The division also oversees various departments' research activities within CyberSecurity Malaysia that aim to shape and influence the nation's cybersecurity strategic environment and coordinate research collaborations with other research institutions, higher learning institutions and private sectors. Together, this will create the synergy for a successful Research and Development in information security.

The Research Division has three departments namely;

1. Strategic Research and Advisory (SRA),
2. Knowledge Management Center (KMC); and
3. Cyber Action & Intelligence Team (CAIT)

Strategic Research and Advisory aims to produce high quality research and studies papers in the field of information security as one of the reliable sources for decision makers at the strategic level. We also provide strategic advice and feedback to stakeholders' enquiries on cyber security matters. In addition, we spearhead and establish new initiatives - such as collaborations with relevant local and international parties, and implementation of cyber security technologies.

Your **cyber safety** is our **concern**

MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

CyberSecurity Malaysia
(726630-U)

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

T: +603 - 8800 7999
F: +603 - 8008 7000
E: info@cybersecurity.my

Customer Service Hotline:
1 300 88 2999
www.cybersecurity.my

Securing Our Cyberspace

CyberSecurity Malaysia is the national cybersecurity specialist and technical agency committed to provide a broad range of cybersecurity innovation-led services, programmes and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace. Among specialised cyber security services provided are Cyber Security Responsive Services; Cyber Security Proactive Services; Outreach and Capacity Building; Strategic Study and Engagement, and Industry and Research Development.

For more information, please visit
www.cybersecurity.my

For general inquiry, please email to
info@cybersecurity.my

Stay connected with us on

f CyberSecurityMalaysia
in CyberSecurity Malaysia
X cybersecuritymy
cybersecurity_my
cybersecuritymy

CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis
Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan
Malaysia

Tel: +603 8800 7999
Fax: +603 8008 7000
Email: info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

@cybersecuritymy
CyberSecurityMalaysia
cybersecurity_malaysia
CyberSecurityMy

MINISTRY OF DIGITAL