Conference Program

Sunday, 24 June
Pre-Conference

Monday, 25 June
SABAH | Management Track
SARAWAK
KEDAH+SELANGOR
PERAK | Workshop
MELAKA | Other Meeting
JOHOR 1+4 | SIG Meetings

Tuesday, 26 June
SABAH | Management Track
SARAWAK | Tech./ProdSec./Vul. Track
KEDAH+SELANGOR | Technical Track
PERAK | Workshop
MELAKA | Other Meeting
JOHOR 1+4 | SIG Meetings

Wednesday, 27 June
SABAH | Management Track
SARAWAK | Technical Track
KEDAH+SELANGOR | Technical Track
PERAK | Workshop
MELAKA | Other Meeting
JOHOR 1+4 | SIG Meetings

Thursday, 28 June
SABAH | Management/Privacy Track
SARAWAK | Technical Track
KEDAH+SELANGOR | Technical Track
PERAK | Workshop
MELAKA | Other Meeting
JOHOR 1+4 | SIG Meetings

Friday, 29 June
SABAH | Management Track
KEDAH+SELANGOR
MELAKA
PERAK | Workshop
SARAWAK | Other Meetings

Saturday, 30 June
SARAWAK | Other Meetings

Sunday, 24 June

	Pre-Conference
08:00 – 10:00	Registration
10:00 – 17:00	FIRST Hackathon - Melaka Room
14:00 – 19:00	Amazon & FIRST Security Jam - Saboh Room Registration *14:00 – 20:00*
18:30 – 19:00	Newbie Reception - Basement II Foyer
19:00 – 21:00	Ice Breaker Reception - Basement II Foyer

Monday, 25 June

	SABAH Management Track	SARAWAK	KEDAH+SELANGOR	PERAK Workshop	MELAKA Other Meeting	JOHOR 1+4 SIG Meetings
08:00 – 17:00	Registration					
09:00 – 09:45	Opening Remarks					
09:45 – 10:45	**Keynote: The Evolution of the Cyber Threat, Our Response and the Role of Diplomacy** *Christopher Painter (Commissioner, Global Commission on the Stability of Cyberspace)*					
10:45 – 11:15	Networking Break					VRDX SIG Meeting *10:45-12:15*
11:15 – 12:15	**The Road to (IR) Nirvana** *Rob Lowe (Red Hat, AU)*	**A Brief History of p0wn4ge: 18 Years and 4506 Incidents** *Aashish Sharma, Jay Krous (Lawrence Berkeley National Lab, US)*	**Social Mining of Threat Actor Activities** *Fyodor Yarochkin (Trend Micro, TW)*			
12:15 – 12:45	**Learning from chaos, cloud and scale: Netflix SIRT** *Alex Maestretti, Swathi Joshi (Netflix, US)*	**New Types of Attacks: The Evolution of Ransomware as a Service** *Susan Ballestero Rosales (BsidesSJO, CR)*	**The Benefits of an Early Warning System in the Brazilian Academic Network** *Edilson Lima, Rildo Souza (RNP, BR)*			Cyber Threat Intel SIG Meeting *12:15 – 13:45*
12:45 – 14:00	Lunch					
14:00 – 15:00	**Security Response Survival Skills** *Ben Ridgway (Microsoft, US)*	**Mind Hunter - Adversary Inception** *Daniel Hatheway, Levi Gundert (Recorded Future, US)*	**Exploit Kit Hunting with Cuckoo Sandbox** *Andres Elliku (CERT-EE / Estonian Information System Authority, EE); Jurriaan Bremer (Cuckoo Sandbox, NL)*	**IPv6 Security** *Frank Herberg (SWITCH-CERT, CH)* *14:00 – 15:30*		Ethics SIG Meeting *14:00 – 15:30*
15:00 – 15:30	**Cyber Weather - Situational Awareness Product For Our Non-technical Constituents** *Tomi Kinnari (NCSC-FI (National Cyber Security Centre) / Finnish Communications Regulatory Authority, FI)*	**Real-time Log Analysis Tool with STIX 2.0** *Mariko Fujimoto, Takuho Mitsunaga, Wataru Matsuda (The University of Tokyo, JP)*	**The Analysis of DDoS Attack Resources in China** *Han-Bing Yan, Hao Zhou, Jian Xu, Tian Zhu (CNCERT, CN)*			
15:30 – 16:00	Networking Break					Capture the Flag SIG *15:30 – 16:30*
16:00 – 16:30	**Incident Management - The Art of Herding Cats** *Paul Clayton (BT, GB)*	**Proactive Cyber Defense through Attack Modeling and Threat Intelligence** *Hamed Khiabani (Experian, MY)* *16:00 – 17:00*	**Malware Reweaponization - A Case Study** *Karlis Podins (CERT.LV, LV)*	**Not Just Indicators: Data Processing with n6** *Paweł Pawliński (CERT Polska / NASK, PL)* *16:00 – 17:30*	FIRST Update: Financial & Business Review *16:00 – 17:15*	
16:30 – 17:30						Metrics SIG Meeting

Tuesday, 26 June

	SABAH Management Track	SARAWAK Tech./ProdSec./Vul. Track	KEDAH+SELANGOR Technical Track	PERAK Workshop	MELAKA Other Meeting	JOHOR 1+4 SIG Meetings
08:30 – 17:15	Registration					
09:00 – 09:15	Opening Remarks					
09:15 – 10:30	**Keynote: How to Avoid Having a Really Bad Day** *Rob McMillan (Research Director, Gartner)*					
10:30 – 11:00	Networking Break with Exhibitors			**Memory Forensics in Incident Response and Threat Hunting** *Josh Lemon (SANS Institute, AU)* *10:30 – 12:30*		Academic Security SIG Meeting *10:30 – 14:00*
11:00 – 12:00	**An Internet of Governments: How Policymakers Became Interested in "Cyber"** *Klee Aiken (APNIC, AU); Maarten Van Horenbeeck (Maarten Van Horenbeeck, US)*	**Coordinating Vulnerability Disclosure with Multiple Vendors** *Laurie Tyzenhaus (SEI CERT, US)*	**Taking the Attacker Eviction Red Pill** *Frode Hommedal (Telenor, NO)*			
12:00 – 12:30	**Motivating to Successful Collaboration with Results** *Lasse Laukka (Ericsson PSIRT, FI)*	**Removing the Pain From the Repetitive Processing of Vulnerability Reports Using a Vulnerability Ontology** *Masanobu Katagi, Takayuki Uchiyama (JPCERT/CC, JP); Masaki Kubo (NICT, JP)*	**Discovering Evasive Code in Malicious Websites with High- and Low-interaction Honeyclients** *Yuta Takata (NTT-CERT, JP)*			
12:30 – 13:45	Lunch					
13:45 – 14:45	**Improving Threat Intelligence Platform and Information Sharing by Measuring Real-Time Collaboration in TIP like MISP** *Raphaël Vinot (CIRCL, LU)*	**Mature PSIRTs Need Mature Tools** *Beverly Finch (Lenovo PSIRT, US)*	**Building and Maintaining Large-scale Honeypot Sensor Networks** *Piotr Kijewski (The Shadowserver Foundation, PL)*	**Reigning in the Raw Power of PyMISP Thanks to Python** *Steve Clement (CIRCL, LU)* *13:45 – 15:30*		
14:45 – 15:45	**Outside the Box - Training Through Surprise** *Frode Hommedal (Telenor, NO)*	**"Moving to The Left": Getting Ahead of Vulnerabilities by Focusing on Weaknesses** *Jim Duncan (Jim Duncan, US)*	**Deep Dive: Case Study Responding to Intrusions into the US Electric Sector** *Jermaine Roebuck, Mark Bristow (DHS Hunt and Incident Response Team, US)*			Red Team SIG Meeting *14:30-16:00*
15:45 – 16:15	Networking Break with Exhibitors					
16:15 – 17:15	**Internet Cartography using BGP and the Implications to Data Sovereignty** *Fyodor Yarochkin (Trend Micro, TW)*	**A holistic approach to ensure product security** *Christer Stenhäll (Ericsson PSIRT, FI)*	**Threat Hunting Techniques at Scale** *Dhia Mahjoub, Thomas Mathew (Cisco Umbrella (OpenDNS), US)*	**Catching Up with Osquery Workshop** *Douglas Wilson (Uptycs, US)* *16:15 – 17:50*	Lightning Talks *16:15 – 17:45*	ICS SIG Meeting *16:00-17:00*
17:15 – 19:15	Vendor Show Case - Basement II Foyer					

Wednesday, 27 June

	SABAH Management Track	SARAWAK Technical Track	KEDAH+SELANGOR Technical Track	PERAK Workshop	MELAKA Other Meeting	JOHOR 1+4 SIG Meetings
08:30 – 15:45	Registration					
09:00 – 09:15	Opening Remarks					
09:15 – 10:30	**Keynote: Jury-Rigging Democracy: The Crazy, Sad Saga of Election Security in the U.S.** *Kim Zetter (Cybersecurity Journalist and Author)*					
10:30 – 11:00	Networking Break with Exhibitors			**What's Up DOCX?: Malicious Office Document Evolution Study** *Mahmud Ab Rahman (Netbytesec sdn bhd, MY)* *10:30 – 12:30*		Vulnerability Coordination SIG Meeting *10:30 – 12:30*
11:00 – 11:30	**Civil Society Under Attack - Trends and Tactics** *Daniel Bedoya (Access Now, CR); Szeming Tan (Security Consultant, MY)*	**Patchwork : From One Malicious Document to Complete TTPs of a Medium Skilled Threat Actor** *Daniel Lunghi (Trend Micro, FR); Jaromir Horejsi (Trend Micro)*	**Why is CTI Automation harder than it needs to be.. and what can security teams do about it.** *Allan Thomson (LookingGlass Cyber Solutions, US)*			
11:30 – 12:30	**Preparing the Village - Lessons Learned in Cross-Industry Vulnerability Disclosure** *Phillip Misner (Industry Consortium for the Advancement of Security on the Internet (ICASI), US)*	**Behind the Scenes of Recent Botnet Takedown Operations** *David Watson (The Shadowserver Foundation, GB)*	**Securing your in-ear fitness coach: Challenges in hardening next generation wearables** *Sumanth Naropanth, Sunil Kumar (Deep Armor, IN)*			
12:30 – 13:45	Lunch					Passive DNS Exchange SIG Meeting *13:00-14:00*
13:45 – 14:15	**Free BugBounty as a CERT** *Emilien Le Jamtel (CERT-EU, BE)*	**Banks and Russian Speaking Adversaries** *Alexander Kalinin (CERT-GIB (Group-IB), RU)*	**Detect & Respond to IoT Botnets as an ISP** *Christoph Giese (Telekom Security, DE)*	**Semi-Automated Cyber Threat Intelligence (ACT)** *Martin Eian (mnemonic, NO)* *13:45 – 16:45*		
14:15 – 15:15	**Scaling Up Security to the Whole Country** *Martijn van der Heide (ThaiCERT, TH)*	**Crawl, Walk, Run: Living the PSIRT Framework** *Mark Stanislav (Duo Security, US)*	**Things Attack: Peek into an 18-month IoT Honeypot** *Tan Kean Siong (The Honeynet Project, MY)*		Lightning Talks *14:15 – 16:00*	Vendor SIG Meeting *14:00-17:00*
19:00 – 22:00	Conference Banquet - All Attendees Welcome! - Grand Ballroom					

Thursday, 28 June

	SABAH Management/Privacy Track	SARAWAK Technical Track	KEDAH+SELANGOR Technical Track	PERAK Workshop	MELAKA Other Meeting	JOHOR 1+4 SIG Meetings
08:30 – 17:00	Registration					
09:00 – 09:15	Opening Remarks					
09:15 – 10:30	**Keynote: Lessons Learned From a Man-in-the-Middle Attack** *Frank Groenewegen (Chief Security Expert, Fox-IT) & Erik de Jong (Chief Research Officer, Fox-IT)*					
10:30 – 11:00	Networking Break with Exhibitors			**Hands-on exploitation and hardening of wearable and IoT platforms** *Sumanth Naropanth, Sunil Kumar (Deep Armor, IN)* *10:30 – 12:30*		
11:00 – 12:00	**Don't Ignore GDPR; It Matters Now!** *Thomas Fischer (Independent, GB)*	**Malvertising: an Italian Tale** *Andrea Minigozzi, Antonio Rossi (Leonardo Spa, IT)*	**What's in a Name? The Need for Global Identifiers of Badness.** *Richard Struse (The MITRE Corporation, US)*			Traffic Light Protocol SIG Meeting *11:00-12:00*
12:00 – 12:30	**What was in that Data?** *Gant Redmon (IBM Resilient, US)*	**A little tour in the world of password stealers** *Paul Jung (Excellium Services, LU)*	**The Andromeda Botnet Takedown** *Benedict Addis (Shadowserver / Registrar of Last Resort (RoLR), GB)*			
12:30 – 13:45	Lunch					Big Data SIG Meeting *12:45-14:45*
13:45 – 14:15	**Security and Privacy Incident Response at Ericsson** *Thomas Grenman (Ericsson, FI)*	**Determining the Fit and Impact of CTI Indicators on your Monitoring Pipeline (TIQ-Test 2.0)** *Alex Pinto (Niddel (a Verizon Company), US)* *13:45 – 14:45*	**TLP to IEP Evolution: What, Why & How** *Tom Millar (US-CERT, US)* *13:45 – 14:45*	**Red Team vs Blue Team Tabletop Exercise and Random Scenario Creation Using Cards** *Chiyuki Matsuda (DeNA Co., Ltd., JP); Mitsuru Haba (Canon Inc., JP); Satoshi Yamaguchi (NTT, JP); Takashi Kikuta (transcosmos Inc., JP); Yoshihiro Masuda (Fuji Xerox Co., Ltd., JP); Yusuke Kon (Trend Micro Inc., JP)* *13:45 – 15:15*	Lightning Talks *13:45 – 15:15*	
14:15 – 14:45	Panel: Q&A on Privacy *Andrew Cormack - Moderator (Jisc, GB); Gant Redmon (IBM Resilient, US); Thomas Fischer (Independent, GB)*					
14:45 – 15:15	**Managing Risks Through Taxonomies** *Serge Droz (Open Sytems AG, CH)*	**Practical Integration of Threat Intelligence and CSIRT Processes to Accelerate Efficiency and Timely Response of Incidents: Malaysia CERT Case Study** *Sharifah Roziah Mohd Kassim, Syazwan Hafizzudin Shuhaimi (CYBERSECURITY MALAYSIA, MY)*	**Multi-dimensional Malware Similarity will let you Catch Up with Malware Developers** *Koji Yamada, Kunihiko Yoshimura, Ryusuke Masuoka, Toshitaka Satomi (Fujitsu System Integration Laboratories Limited, JP)*			
15:15 – 15:45	Networking Break with Exhibitors					
15:45 – 17:45	Annual General Meeting (FIRST Members Only) - Sabah Room					

Friday, 29 June

	SABAH Management Track	KEDAH+SELANGOR	MELAKA	PERAK Workshop	SARAWAK Other Meetings
08:00 – 11:00	Registration				
08:30 – 08:45	Opening Remarks				
08:45 – 09:45	**Keynote: 30 years on...why are we still needed more than ever?** *Paul Jackson (Managing Director, Kroll)*				
09:45 – 10:00	Networking Break			**STIX2/TAXII2 Workshop** *Allan Thomson (LookingGlass Cyber Solutions, US); Richard Struse (The MITRE Corporation, US); Trey Darley (New Context, BE)* *09:45 – 12:30*	
10:00 – 10:30	**Collaborative National-level Incident Response Model to Address Large-Scale Data Breach Attack in Malaysia** *Farah Ramlee, Kilausuria Abdullah (Cybersecurity Malaysia, MY); Sharifah Roziah Mohd Kassim (CYBERSECURITY MALAYSIA, MY)*	**Professionalizing the Field of Cybersecurity Incident Response** *Tom Millar (US-CERT, US)* *10:00 – 11:00*	**Attacker Antics: Illustrations of Ingenuity** *Bartosz Inglot, Vincent Wong (FireEye, SG)* *10:00 – 11:00*		
10:30 – 11:00	**Creating NIS Compliant Country in a Non-regulated Environment, Case Study Croatia** *Jurica Cular (ISSB, HR)*				
11:00 – 12:00	**Bridging Cultures: Collaboration of the US/Global and Japanese Financial Communities** *Natsuko Inui (Financial Services Information Sharing and Analysis Center (FS-ISAC), JP)*	**Exposing Crypto Phishing BulletProof Hosting** *Artsiom Holub, Austin McBride (Cisco Umbrella, US)*	**Emotet Malware** *Neil Fox (BT Security, GB)*		
12:00 – 12:45	Closing Remarks & Raffle Drawings				
12:45 – 13:45	Lunch				
14:00 – 18:00	13th Annual Technical Meeting for CSIRTs with National Responsibility (invitation only) *SARAWAK*				
18:00 – 19:30					13th Annual Technical Meeting for CSIRTs with National Responsibility Reception (invitation only)

Saturday, 30 June

	SARAWAK Other Meetings
08:00 – 17:00	13th Annual Technical Meeting for CSIRTs with National Responsibility (invitation only) *SARAWAK*

Sponsorship Team

Local host

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

CyberSecurity MALAYSIA

Local Convention Bureau Support

Ministry of Tourism and Culture Malaysia

Malaysia Convention & Exhibition Bureau

Diamond Sponsor

Microsoft

Platinum Sponsor

Alibaba Group

POLYSWARM

VMRAY

aws

Gold Sponsor

NC4

BITSIGHT

Google

Booz | Allen | Hamilton

RAPID7

ANOMALI

OneTrust
Privacy Management Software

Silver Sponsor

insignary

Arctic Security

DOMAINTOOLS

Recorded Future

FIRST JapanTeams

Network Sponsor

CISCO

Internet Sponsor

TIME

Banquet Sponsor

IBM Resilient

Ice Breaker Reception Sponsor

SUREVINE

Supporting Sponsor

CIRCL
Computer Incident Response Center Luxembourg

Google

HITACHI

NC4

Exhibitors Sponsor

Alibaba Group

ANOMALI

Arctic Security

aws

Booz | Allen | Hamilton

BITSIGHT

CISCO

CyberSecurity MALAYSIA

DOMAINTOOLS

eclectic iq

IBM Resilient

insignary

ISACA
Trust in, and value from, information systems

Microsoft

CYSECA

NC4

OneTrust
Privacy Management Software

POLYSWARM

RAPID7

Recorded Future

RISKIQ

SANS

SUREVINE

TIME

VMRAY