CONFERENCE PROGRAM

Overview

Sunday, 11 June
Pre-Conference

Monday, 12 June
San Geronimo B | Management Track
San Geronimo A | Technical Track
San Geronimo C | Technical Track
Auditorium | Team Insights
Flamingo A-B | Other Meetings

Tuesday, 13 June
Auditorium | Management Track
San Geronimo A | Technical Track
San Geronimo C | Technical Track
San Geronimo B | Team Insights
Flamingo A-B | Other Meetings

Wednesday, 14 June
Auditorium | Management Track
San Geronimo A | Technical Track
San Geronimo C | Technical Track
San Geronimo B | Team Insights
Flamingo A-B | Other Meetings

Thursday, 15 June
Auditorium | Management Track
San Geronimo A | Technical Track
San Geronimo C | Technical Track
San Geronimo B | Team Insights
Flamingo A-B-C-D | Other Meetings

Friday, 16 June
Auditorium | Management Track
San Geronimo A | Technical Track
San Geronimo C | Technical Track
San Geronimo B | Team Insights
Flamingo A-B | Other Meetings

Saturday, 17 June
Other Meetings

Sunday, 11 June

	Pre-Conference
08:00 – 10:00	Registration
11:00 – 17:00	**FIRST Hackathon** - Flamingo A
14:00 – 19:00	**FIRST & Amazon Security Jam Orientation** - Tropical Ballroom
18:30 – 19:00	Newbie Reception - Atlantic Garden
19:00 – 21:00	Ice Breaker Reception - Atlantic Garden

Monday, 12 June

	San Geronimo B Management Track	San Geronimo A Technical Track	San Geronimo C Technical Track	Auditorium Team Insights	Flamingo A-B Other Meetings
08:00 – 17:00	Registration				
09:00 – 09:45	Opening Remarks				
09:45 – 10:45	Keynote: Detection, Investigation and Response at Billion Person Scale Alex Stamos (Facebook)				
10:45 – 11:15	Coffee Break				Red Team SIG Meeting 10:45 – 12:15
11:15 – 12:00	**Measuring Similarity Between Cyber Security Incident Reports** Samuel Perl, Zachary Kurtz (Software Engineering Institute, US)	**Beyond Matching: Applying Data Science Techniques to IOC-based Detection** Alex Pinto (Niddel, US)	**CSIRT Under Attack** Riccardo Tani (Si Cyber Consult, AE)	**Windows Credentials, Attacks, and Mitigation Techniques** Chad Tilbury (SANS Institute, US) 11:15 – 12:45	
12:00 – 12:45	**Active Directory : How To Change a Weak Point Into a Leverage for Security Monitoring** Vincent Le Toux (Engie, FR)	**IoCannon: Blasting Back on Attackers with Economics -or- How do we Improve the Power of IoCs?** Eireann Leverett (Concinnity Risks, GB); Marion Marschalek (Independant, AT)	**The Ransomware Odyssey: Their Relevance and Their Kryptonite** Marco Figueroa, Ronald Eddings (Intel Corporation, US); Sue Ballestero (Intel, CR)		
12:45 – 14:00	Lunch Break				Ethics SIG Meeting 12:45 – 15:00
14:00 – 14:45	**Building a High Performing Cyber Security Team on the Cheap** Christopher Payne (Target, US)	**Threat Ontologies for Cyber Security Analytics** Dr. Martin Eian (mIRT/mnemonic AS, NO)	**Cyber Terrorist Activity: The New Way to Cause Chaos** Kyle Wilhoit (DomainTools, US)	**OSS Security: That's Real Mature Of You!** Christine Gadsby (BlackBerry, US); Jake Kouns (Risk Based Security, US) 14:00 – 15:30	
14:45 – 15:30	**Building a Product Security Team-The Good, the Bad and the Ugly - Lessons from the Field** Peter Morin (Forcepoint, CA)	**Best Practices for Building a Large Scale Sensor Network** Juhani Eronen (NCSC-FI / FICORA, FI)	**Are West African Cybercriminals on Safari in your Network?** David Sancho (Trend Micro, ES)		
15:30 – 16:00	Coffee Break				
16:00 – 16:30	**Trying to Know Your Own Backyard (A National CERT Perspective)** Paweł Pawliński (CERT Polska / NASK, PL)	**WatchEvaluateEnrichPunch (WEEP): A Poor Man's Self-Defence Host Monitor.** Adrian Sanabria (Savage Security, US); Konrads Smelkovs (KPMG LLP, GB)	**SDN Control System Based on Threat Level of Shared Information** Takuho Mitsunaga (The University of Tokyo, JPCERT/CC, JP)	FIRST Update: Financial & Business Review FIRST Members Only 16:00 – 17:00	Information Exchange Policy SIG Meeting 16:00 – 17:00
16:30 – 17:00	**Digital Supply Chain: The Exposed Flank In 2017** Martin McKeay (Akamai, US)	**AIL Framework - Analysis Information Leak Framework** Alexandre Dulaunoy, Steve Clement (CIRCL - Computer Incident Response Center Luxembourg, LU)	**HIRT Locker 2.0 - Next Generation Hunting** Christopher Butera (US-CERT, US)		

Tuesday, 13 June

	Auditorium Management Track	San Geronimo A Technical Track	San Geronimo C Technical Track	San Geronimo B Team Insights	Flamingo A-B Other Meetings
08:30 – 17:30	Registration				
09:30 – 09:45	Opening Remarks				
09:45 – 10:45	**Keynote: A Decade of Lessons in Incident Response** Darren Bilby (Google, AU)				
10:45 – 11:15	Coffee Break				Malware Analysis SIG Meeting 10:45 – 12:45
11:15 – 11:45	**Communicating Risk: A Comparative Approach to Vulnerability Remediation** Mark-David Mclaughlin (Cisco, US)	**Hunting for Threats in Academic Networks** Fyodor Yarochkin (Trend Micro, TW); Vladimir Kropotov (Trend Micro, RU)	**Practical Workflow for Automation and Orchestration of Addressing Cyber. Threat: Case Study of Mirai Botnet in Malaysia** Megat Muazzam Abdul Mutalib (CyberSecurity Malaysia, MY)	**Change is the Only Constant: The Progression of Detection and Response at Google** Fatima Rivera (Google, US) 11:15 – 12:00	
11:45 – 12:15	**The Arrr in PSIRT** Beverly Finch (Lenovo, US)	**Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification** Ben Stock, Christian Rossow (CISPA, DE)	**Panel Topic: Mirai: How Did We Do?** Chris Baker (Dyn, US); Martin McKeay (Akamai, US); Megat Muazzam Bin Abdul Mutalib (MyCERT, MY); Merike Kaeo (Farsight Security, US); Yiming Gong (Qihoo 360, CN) 11:45 – 12:45		
12:15 – 12:45	**Web as ongoing threat vector: case studies from Europe and Asia Pacific** Fyodor Yarochkin (Trend Micro, TW); Vladimir Kropotov (Trend Micro, RU)	**Experiences and Lessons Learned from a Siemens-Wide Security Patch Management Service for Products** Manuel Ifland (Siemens AG, DE)		**Trust Nothing: Google's Approach to Enterprise Security in Forensic Context** Jan Monsch (Google, CH)	
12:45 – 14:00	Lunch Break				
14:00 – 14:45	**Things That Make You Go HMM: Using a Simple Hunting Maturity Model to Establish and Improve your Threat Hunting Program** David J. Bianco (Target, US)	**Advanced Incident Detection and Threat Hunting using Sysmon (and Splunk)** Tom Ueltschi (Swiss Post, CH)	**Dismantling the Avalanche Botnet** Kaspar Clos (CERT-Bund / BSI, DE)	**Privacy Incident Management: It's Not Just Security Any More** Andy Bohm (Google, US)	VRDX SIG Meeting 14:00 – 15:30
14:45 – 15:30	**Building a Threat Hunting Framework for the Enterprise** Joseph Ten Eyck (Target Company, US)	**Defensive Evasion: How APT Adversaries Bypass Security Controls** Aaron Shelmire (SecureWorks, US)	**Disrupting IoT Worms in Finland (2016 Edition)** Markus Lintula (NCSC-FI / FICORA, FI)	**Remediation Ballet: Choreographing Your Team To Victory** Matt Linton (Google, US)	
15:30 – 16:00	Coffee Break				
16:00 – 16:30	**These Aren't The IR Processes You're Looking For** Jake Kouns (Risk Based Security, US)	**Malicious Proxy Auto-Configs: Harvesting Credentials From Web Forms Made Easy** Jan Sirmer, Jaromir Horejsi (Avast Software, CZ)	**Hajime & the Mainline DHT** Kevin O'Sullivan (BT Plc, GB)	**Finding An Intruder in a 10TB Haystack: The Benefits of Similarity Searching** Thomas Dullien (Google, CH) 16:00 – 16:45	Information Sharing SIG Meeting 16:00 – 17:00
16:30 – 17:00	**From Bullet Journal to Lessons Learned: How to Manage Coordination and Cooperation Development in Ad-hoc Working Environment?** Jarna Hartikainen (NCSC-FI, FI)	**Collaborative Information Sharing Model for Malware Threat Analysis** Aswami Ariffin (CyberSecurity Malaysia, MY)	**Panel Topic Friend or Foe? Named Flaws, the Impact to Your Products and Your Customers** Amy Rose, Beverly Finch (Lenovo, US); Art Manion (CERT Coordination Center (CERT/CC), US); Lisa Bradley (NVIDIA, US) 16:30 – 17:30		
17:00 – 17:30	**Revising the TLP - Lessons Learned** Don Stikvoort (Open CSIRT Foundation, NL)	**Countering Innovative Sandbox Evasion Techniques Used by Malware** Carsten Willems, Frederic Besler (VMRay, DE)		Q/A with speakers	
17:30 – 19:30	Vendor Show Case				

Wednesday, 14 June

	Auditorium Management Track	San Geronimo A Technical Track	San Geronimo C Technical Track	San Geronimo B Team Insights	Flamingo A-B Other Meetings
08:00 – 09:15					Passive DNS Exchange SIG Meeting
08:30 – 17:00	Registration				
09:30 – 09:45	Opening Remarks				
09:45 – 10:45	**Keynote: Cybersecurity and the Age of Privateering** Florian Egloff (University of Oxford, GB)				
10:45 – 11:15	Coffee Break				
11:15 – 12:00	**Ozon: Running a Gap Bridging Cybercrisis Exercise** Remon Klein Tank (SURFcert, NL)	**Update on PSIRT/CSIRT Services Framework** Peter Allor (IBM, US) 11:15 – 12:45	**THINKPWN: PSIRT Case Study of a Zero-Day** Amy Rose (Lenovo, US)	Q/A Roundtable with Google's Security and Privacy team 11:15 – 12:45	Metrics SIG Meeting *(meeting ends 13:15)* Room: Flamingo CD 11:15 – 12:45
12:00 – 12:45	**Steel Sharpens Steel: Using Red Teams to Make Blue Teams Better** Christopher Payne (Target, US)		**The Budding World of Cloud Storage Abuse and Exploitation : A Technical Deep Dive** Aditya K Sood (BlueCoat, A Symantec Company, US)		
12:45 – 14:00	Lunch Break				Vendor SIG Meeting 12:45 – 14:15
14:00 – 14:45	**How To Ruin Your Weekend (And Business) In Few Simple Steps** Przemek Jaroszewski (CERT Polska/NASK, PL)	**A Look into the Long Tale of Cyber Threats** Eyal Paz, Gadi Naveh (Check Point, IL)	**You're Leaking: Incident Response in the World of DevOps** Levi Gundert (Recorded Future, US)	**Managerial Strategies for Improving the Social Maturity of Cybersecurity Incident Response Teams and Multiteam Systems: A Workshop** Daniel Shore, Stephen Zaccaro (George Mason University, US) 14:00 – 15:30	
14:45 – 15:30	**Handling an Incident in CERT-EU** Emilien Le Jamtel (CERT-EU, BE)	**Going Undetected: How Cybercriminals, Hacktivists, and Nation States Misuse Digital Certificates** Kevin Bocek (Venafi, US)	**The Incident Responder and the Half Year APT** Dr. Martin Eian, Jon Røgeberg (mIRT/mnemonic AS, NO)		Vulnerability Coordination SIG Meeting Room: Flamingo CD 14:45 – 16:00
15:30 – 16:00	Coffee Break				
16:00 – 17:00	Lightning Talks	**Panel Topic: Incident Response Providers: Casework Trends** Brian Klenke (Morphick, US); Eric Szatmary (SecureWorks, US); Robert Floodeen (PwC, US)	**Panel Topic: Issues Surrounding Internet of Things (IoT) Security Upgradibility and Patching** Allan Friedman (National Telecommunications and Information Administration, US); John Banghart (Venable LLP, US); Kent Landfield (McAfee, US); Vic Chung (SAP, CA)	**WannaCry: What can we do better?** Paul Vixie (Farsight Security, US); Saâd Kadhi (Banque de France, FR)	ICS SIG Meeting
19:00 – 22:00	Conference Banquet - All Attendees Welcome!				

Thursday, 15 June

	Auditorium Management Track	San Geronimo A Technical Track	San Geronimo C Technical Track	San Geronimo B Team Insights	Flamingo A-B-C-D Other Meetings
08:30 – 17:00	Registration				
09:30 – 09:45	Opening Remarks				
09:45 – 10:45	**Keynote: 18 Years Old, it's Time to Become Mature** Martijn de Hamer (NCSC-NL, NL)				
10:45 – 11:15	Coffee Break				
11:15 – 12:00	**How to Become a Mature CSIRT in 3 Steps** Don Stikvoort (Open CSIRT Foundation, NL); Mirosław Maj (Open CSIRT Foundation, PL)	**Canaries in a Coal Mine...** Peter Morin (Forcepoint, CA)	**When Phone Networks Go Down - Who You Gonna Call?** Mikko Karikytö (Ericsson, FI)	**DNS is NOT Boring! Using DNS to Expose and Thwart Attacks** Rod Rasmussen (Infoblox, US) 11:15 – 12:45	Intro to CVSS
12:00 – 12:45	**What Metrics Should a CSIRT Collect to Measure Success (Or What Questions Should We Be Asking and How Do We Get the Answers?)** Robin Ruefle (CERT Division, SEI, CMU, US)	**Lean Gains - Small Team Effectiveness** Ben May (AEMO, AU)	**You Don't Need a Better Car, You Need to Learn How to Drive: On the Importance of Cyber-Defense Line Automation.** Enrico Lovat, Florian Hartmann, Philipp Lowack (Siemens CERT, DE)		CVSS General meeting (open meeting)
12:45 – 14:00	Lunch Break				CVSS SIG (closed meeting)
14:00 – 14:45	**Medical Device Security: A Sucking Chest Wound That Needs Emergency Medicine** Denise Anderson (NH-ISAC, US)	**Blackhole Networks - an Underestimated Source for Information Leaks** Alexandre Dulaunoy (CIRCL, LU)	**TheHive: a Scalable, Open Source and Free Incident Response Platform** Saâd Kadhi (Banque de France, FR)	**The Art of the Jedi Mind Trick: Learning Effective Communication Skills** Jeff Man (Cybrary.it, US) 14:00 – 15:30	
14:45 – 15:30	**Embodied Vulnerabilities: Compromising Medical Implants** Eireann Leverett (Concinnity Risks, GB); Marie Moe (SINTEF, NO)	**Improving Network Intrusion Detection with Traffic Denoise** Miroslav Stampar (Information Systems Security Bureau, HR)	**Marvin: Automated Incident Handling at DFN-CERT** Eugene Brin, Jan Kohlrausch (DFN-CERT, DE)		
15:30 – 16:00	Coffee Break				
16:00 – 18:00	FIRST Annual General Meeting FIRST Members Only				

Friday, 16 June

	Auditorium Management Track	San Geronimo A Technical Track	San Geronimo C Technical Track	San Geronimo B Team Insights	Flamingo A-B Other Meetings
09:00 – 11:00	Registration				
09:30 – 09:45	Opening Remarks				
09:45 – 10:45	**Keynote: Post-Quantum Cryptography** Brian Lamacchia (Microsoft Research, US)				
10:45 – 11:15	Coffee Break				**Trainer Training** 10:45 – 17:45
11:15 – 11:45	**PyNetSim: A Modern INetSim Replacement** Jason Jones (Arbor Networks ASERT, US)	**Rio 2016 Olympic CSIRT - Creation, Operation and Lessons Learned** Romulo Rocha (Former Rio2016 Commitee and now Tempest Security Intelligence, BR)	**Deep Learning for Incident Response: Predicting and Visualizing Cyber Attacks Using Open Data, Social Media and GIS** Anne Connell (CERT, US)	**::1 The Official Home for IPv6 Attacks** Josh Porter (McAfee, US); Marco Figueroa, Ronald Eddings (Intel Corporation, US) 11:15 – 12:45	
11:45 – 12:15	**APT Log Analysis - Tracking Attack Tools by Audit Policy and Sysmon -** Shusei Tomonaga (JPCERT/CC, JP)	**Implementing a Country-wide Sensor Infrastructure for Proactive Detection of Malicious Activity** Edilson Lima, Rildo Souza (RNP, BR)	**Improving Useful Data Extraction from Cybersecurity Incident Reports** Matthew Sisk (The CERT Program in the Software Engineering Institute at Carnegie Mellon University, US); Samuel Perl (Software Engineering Institute, US)		
12:15 – 12:45	**Non-Formal - Everything Out of Normal** Svetlana Amberga (CERT.LV, LV)	**Moving Like a Spook Through Walls or Being Just a Shadow for APT Detectors** Dmitry Bestuzhev (Kaspersky Lab, US); Fabio Assolini (Kaspersky Lab, BR)	**Experiences in Threat Data Processing and Analysis Using Open Source Software** Morton Swimmer (Trend Micro, Inc, DE)		
12:45 – 14:00	Closing Remarks				
14:00 – 15:00	Lunch Break National CSIRT meeting (invitation only) 14:00 – 18:00				
18:00 – 19:30	National CSIRT Reception (invitation only)				

Saturday, 17 June

	Other Meetings
08:00 – 17:00	National CSIRT meeting (invitation only)

Sponsorship Team

Local Host

GM Security Technologies

Diamond Sponsor

amazon web services

Platinum Sponsor

Microsoft

Gold Sponsor

Fortinet

Google

NSS Labs

OPSWAT

Recorded Future

VMRay

Silver Sponsor

Anomali

BitSight

Booz | Allen | Hamilton

Coordinat-iR

CyberSponse
Adaptive Security

DomainTools

Forcepoint
powered by Raytheon

NC4

Rapid7

Network Sponsor

Cisco

Internet Sponsor

Claro

Banquet Sponsor

IBM Resilient

Sunday Ice Breaker Reception

Sureview

Security Jam Sponsor

AWS Security

Supporting Sponsors

CIRCL
Computer Incident Response Center Luxembourg

Google

Hitachi

thebestvpn