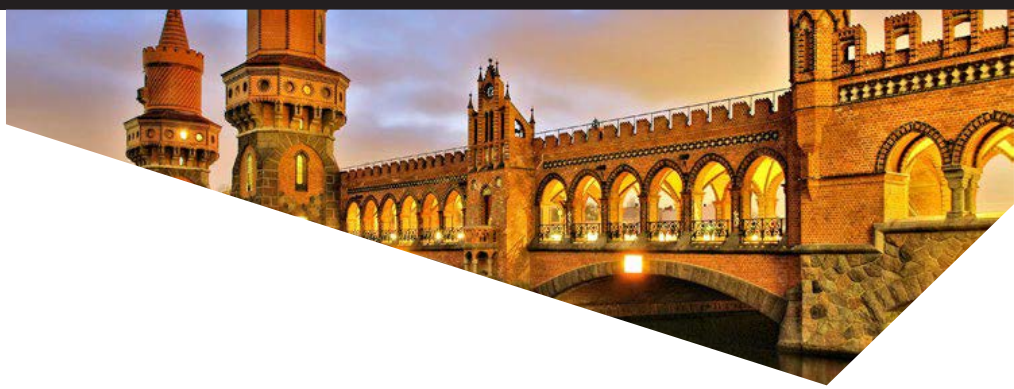
27th ANNUAL FIRST CONFERENCE BERLIN 14-19 JUNE 2015



CONFERENCE **PROGRAM**

Overview

June **13th**, Saturday
Pre-Conference

June **14th**, Sunday
Pre-Conference

June **15th**, Monday
Potsdam I
Potsdam III
Bellevue
Charlottenburg
Other Meetings

June **16th**, Tuesday
Potsdam I
Potsdam III
Bellevue
Charlottenburg
Other Meetings

June **17th**, Wednesday
Potsdam I
Potsdam III
Bellevue
Charlottenburg
Other Meetings

June **18th**, Thursday
Potsdam I
Potsdam III
Bellevue
Charlottenburg
Other Meetings

June **19th**, Friday
Potsdam I
Potsdam III
Bellevue
Other Meetings

June **13th**, Saturday

	PRE-CONFERENCE
10:00 › 17:00	FIRST Education & Training Committee Meeting - Check

June **14th**, Sunday

	PRE-CONFERENCE
09:00 › 16:30	**Train the Trainers - Rook** Don STIKVOORT (Avalon Coaching & NLP), Lauri PALKMETS (ENISA)
09:00 › 17:00	FIRST Training - Check FIRST Education Summit III (Invite Only) - Bellevue
15:00 › 16:00	Session Chair Volunteers Meeting - Knight
17:00 › 18:00	Ambassador Program Training - Rook
18:30 › 19:00	Newbie Reception - Pavillon
19:00 › 21:00	Ice Breaker Reception - Pavillon

June **15th**, Monday

	POTSDAM I	POTSDAM III	BELLEVUE	CHARLOTTENBURG	OTHER MEETINGS
09:15 › 09:30	Conference Opening - Potsdam I				
09:30 › 10:00	**Keynote Presentation: IT Security: Future Challenges for Government, Industry and Society - Potsdam I** Cornelia ROGALL-GROTHE (German State Secretary & Federal Government Commissioner for Information Technology)				
10:00 › 10:30	Morning Networking Break - Conservatory / Potsdam Foyer				
10:30 › 11:00	Behind the Scenes this Week at FIRST - Potsdam I				
11:00 › 12:00	**Adventures in Fighting Cybercrime** Mr. Piotr KIJEWSKI (CERT Polska/NASK)	**A Proposal for Cybersecurity Metrics Through Cyber Green** Yurie ITO (JPCERT), Mr. Wes YOUNG (CSIRT Gadgets)	**Building instantly exploitable protection for yourself and your partners against targeted cyber threats using MISP** Mr. Andras IKLODY (CIRCL)	Cybersecurity R&D - BoF	CVSS - BoF - Chess
12:00 › 13:00	Lunch - LA Café & Pavillon				
13:00 › 14:00	**The Crack in KrakenBOT** Mr. Peter KRUSE (CSIS Security Group A/S)	**I'm Sorry to Inform You...** Mr. Eireann LEVERETT (Cambridge Centre for Risk Studies), Dr. Marie MOE (SINTEF ICT)	**3J4E - JIGSAW, JUMPSTART, JUNCTURE: Three Ways to Enhance Cyber-Exercise-Experience** Mr. Stefan RITTER (National IT-Situation Centre and CERT-Bund, German Federal Office for Information Security BSI)	**BetterCrypto.org Workshop and Hands-on Training** Mr. David DURVAUX (BetterCrypto.org), Mr. Aaron ZAUNER (Azet), Mr. L. Aaron KAPLAN (CERT.at)	
14:00 › 14:30	**So You Want a Threat Intelligence* Function (*But Were Afraid to Ask)** Mr. Gavin REID (Lancope)	**Working Towards the Tokyo 2020 Olympics - Situation in 2015** Ms. Mariko MIYA (CDI-CIRT (Cyber Defense Institute, Inc.) - Japan)	**Everyday Etiquette: Responding to Uncoordinated Disclosures** Ms. Laura RABA (US-CERT)	BetterCrypto.org Workshop and Hands-on Training (cont.)	Vendor - SIG - Chess
14:30 › 15:00	Afternoon Networking Break - Conservatory / Potsdam Foyer				
14:30 › 15:00					Vendor - SIG (cont.)
15:00 › 16:00	**Threat Information Sharing; Perspectives, Strategies, and Threat Scenarios** Mr. Timothy GRANCE (NIST), THOMAS MILLAR (US-CERT), Mr. Pawel PAWLINSKI (CERT Polska / NASK), Mr. Luc DANDURAND (ITU), Sarah BROWN (Fox-IT)	**Malware in Your Pipes: The State of SCADA Malware** Mr. Kyle WILHOIT (Trend Micro)	**Collecting, Analyzing and Responding to Enterprise Scale DNS Events** Mr. Bill HORNE (Hewlett-Packard)	BetterCrypto.org Workshop and Hands-on Training (cont.)	Vendor - SIG (cont.)
16:00 › 17:00	**Barriers and Pathways to Improving the Effectiveness of Cybersecurity Information Sharing Among the Public and Private Sectors** Laura FLETCHER (George Mason University), Kristin M. REPCHICK (George Mason University), Julie STEINKE (George Mason University)	FIRST Update: Financial & Business Review	**Incident Response Programming with R** Mr. Eric ZIELINSKI (Nationwide)		Vendor - SIG (cont.)
17:00 › 17:30	Lightning Talk	FIRST Update: Financial & Business Review (cont.)			
17:30 › 18:00	Lightning Talk (cont.)				

June **16th**, Tuesday

	POTSDAM I	POTSDAM III	BELLEVUE	CHARLOTTENBURG	OTHER MEETINGS
08:45 › 09:00	Opening Remarks - Potsdam I				
09:00 › 09:45	**Keynote Presentation: Securing our Future - Potsdam I** Mikko HYPPONEN (F-Secure)				
09:45 › 10:15	Morning Networking Break - Conservatory / Potsdam Foyer				
10:15 › 11:15	**Fact Tables - A Case Study in Reducing Reactive Intrusion Time-to-Know by 95%** Mr. Jeff BOERIO (Intel Corp.)	**SecAdmin - Mitigating APTs – Tools for the Administrator** Mr. David JONES (Cisco)	**Quality Over Quantity—Cutting Through Cyberthreat Intelligence Noise** Mr. Rod RASMUSSEN (IID)	**CSIRT Info Sharing Workshop** Shari LAWRENCE PFLEEGER (I3P-Dartmouth-GMU-NL-SE (various CSIRTS))	
11:15 › 11:45	**Prepare Your Cybersecurity Team for Swift Containment Post Incident** Mr. Michael HARRINGTON (Fidelis Cybersecurity Solutions)	**A Day in the Life of a Cyber Intelligence Professional** Ms. Katherine GAGNON (World Bank Group)	**Seven Years in MWS: Experiences of the Community Based Data Sharing for Anti-Malware Research in Japan** Dr. Masato TERADA (Hitachi Incident Response Team), Yoichi SHINODA (JAIST), Mitsuhiro HATADA (NTT Communications Corporation)	CSIRT Info Sharing Workshop (cont.)	
11:45 › 12:45	Lunch - LA Café & Pavillon				
12:45 › 13:15	**Overview of South Korea Target Malwares** Mrs. Dongeun LEE (KRCERT/CC, KISA)	**When Business Process and Incident Response Collide: The Fine-Tuning of the IR Program** Ms. Reneaue RAILTON (Duke Medicine)	**Ce1sus: A Contribution to an Improved Cyber Threat Intelligence Handling** Mr. Jean-Paul WEBER (GovCERT.lu)	**Hands-on Network Forensics** Mr. Erik HJELMVIK (FM CERT)	Network Monitoring - SIG - Chess
13:15 › 14:15	**The Cybercrime Evolution in Brazil: An Inside View of Recent Threats and the Strategic Role of Threat Intelligence** Mr. Ricardo ULISSES (Tempest Security Intelligence), Mr. Aldo ALBUQUERQUE (Tempest Security Intelligence)	**Security Operations: Moving to a Narrative-Driven Model** Mr. Joshua GOLDFARB (FireEye)	**Case Study: Creating Situational Awareness in a Modern World.** Mr. Michael MEIJERINK (NCSC-NL)	Hands-on Network Forensics (cont.)	Network Monitoring - SIG (cont.) - Chess
14:15 › 14:45	Afternoon Networking Break - Conservatory / Potsdam Foyer				
14:45 › 15:45	**Enabling Innovation in Cyber Security** Mr. Michael GORDON (Lockheed Martin)	**Technology, Trust, and Connecting the Dots** Mr. George JOHNSON (NC4), Mr. Wayne BOLINE (DIB ISAC (DSIE)), Denise ANDERSON (FS-ISAC)	**Bring Your Own Internet Of Things (BYO-IoT)** Mr. Jake KOUNS (Risk Based Security), Mr. Carsten EIRAM (Risk Based Security)	Hands-on Network Forensics (cont.)	VRDX - SIG - Check
15:45 › 16:45	**DSMS: Automating Decision Support and Monitoring Workflow for Incident Response** Mr. Chris HORSLEY (CSIRT Foundry), Mr. SC LEUNG (HKCERT)	**Crisis Communication for Incident Response** Mr. Scott ROBERTS (GitHub)	**Cyber Security Challenges in the Financial Sector: Internal and External Threats** Ms. Rosa Xochitl SARABIA BAUTISTA (Mnemo-CERT)	Hands-on Network Forensics (cont.)	VRDX - SIG (cont.)
17:00 › 18:00					Energy - SIG - Chess
17:00 › 19:00	Vendor Showcase Reception - Conservatory / Potsdam Foyer				

June **17th**, Wednesday

	POTSDAM I	POTSDAM III	BELLEVUE	CHARLOTTENBURG	OTHER MEETINGS
08:45 › 09:00	Opening Remarks - Potsdam I				
09:00 › 10:00	**Keynote Presentation: Europol's European Cybercrime Centre – punching above its weight - Potsdam I** Philipp AMANN (European Cybercrime Centre, Europol)				
10:00 › 10:30	Morning Networking Break - Conservatory / Potsdam Foyer				
10:30 › 11:30	**Passive Detection and Reconnaissance Techniques to Find, Track and Attribute Vulnerable "Devices"** Mr. Alexandre DULAUNOY (CIRCL - Computer Incident Response Center Luxembourg), Mr. Eireann LEVERETT (Cambridge Centre for Risk Studies)	**Maximizing Value of your Threat Intelligence for Security Incident Response** Mr. Jonathan TOMEK (Lookingglass Cyber Solutions)	FIRST Update: Education & Training	**CVSS v3 Hands-on Training** Mr. Seth HANFORD (TIAA-CREF)	Metrics - SIG - Check (10:30 - 12:30) | CSIRT Basics for Policy Makers BoF - Chess (10:30-12:00)
11:30 › 12:30	**National Cyber Protection through Facilitation. Real Cases by CERT-UA** Mr. Nikolay KOVAL (CERT-UA)	**Traffic Light Protocol (TLP) - BoF** Tom MILLAR (US-CERT)	**Sustainable CSIRTS - SIG** Mr. Jamie LORD (CERT/CC), Tracy BILLS (CERT/CC), Wassie GOUSHE (CERT/CC), Bill JONES (CERT/CC)	CVSS v3 Hands-on Training (cont.)	Metrics - SIG - Check (10:30 - 12:30) cont. | CSIRT Basics for Policy Makers BoF - Chess (10:30-12:00) cont.
12:30 › 13:30	Lunch - LA Café & Pavillon				
13:30 › 14:30	**The Daily Show Agenda** Mr. Chris HALL (Wapack Labs)	**Data-Driven Threat Intelligence: Useful Methods and Measurements for Handling Indicators** Mr. Alexandre PINTO (Niddel), Mr. Alexandre SIEIRA (Niddel)	**Sinfonier: Storm Builder for Security Intelligence** Mr. Fran GOMEZ (Telefonica), Mr. Leonardo AMOR (Telefonica)	**Hands-on Pen Testing iOS Apps** Mr. Kenneth VAN WYK (KRvW Associates, LLC)	**Policy - BoF - Chess** Mr. Don STIKVOORT
14:30 › 15:00	Afternoon Networking Break - Conservatory / Potsdam Foyer				
15:00 › 16:00	**Theory and Practice of Cyber Threat-Intelligence Management Using STIX and CybOX** Dr. Bernd GROBAUER (Siemens)	**The Needle in the Haystack** Mr. Jasper BONGERTZ (Airbus Defence and Space CyberSecurity GmbH)	**How We Saved the Death Star and Impressed Darth Vader** Mr. Matthew VALITES (Cisco CSIRT), Mr. Jeff BOLLINGER (Cisco CSIRT)	Hands-on Pen Testing iOS Apps (cont.)	**CSIRT Maturity Kit - BoF - Chess** Mr. Don STIKVOORT
16:00 › 17:00	**Validating and Improving Threat Intelligence Indicators** Mr. Douglas WILSON (FireEye)	**Malware Analysis Case Study & Experimental Evaluation on the Applicability of Live Forensics for Industrial Control Systems** Mr. Yuji KUBO (CFC), Mr. Kensuke TAMURA (CFC)	**Machine Learning for Cyber Security Intelligence** Mr. Edwin TUMP (NCSC-NL)	Hands-on Pen Testing iOS Apps (cont.)	FIRST Membership Information Session - Check
17:00 › 18:00	Lightning Talks				
18:30 › 19:15	Reception at the Postbahnhof				
19:15 › 22:00	Banquet at the Postbahnhof				

June **18th**, Thursday

	POTSDAM I	POTSDAM III	BELLEVUE	CHARLOTTENBURG	OTHER MEETINGS
09:00 › 09:15	Opening Remarks - Potsdam I				
09:15 › 10:00	**Keynote Presentation: Collaborative Security - Reflections about Security and the Open Internet - Potsdam I** Olaf KOLKMAN (Internet Society)				
10:00 › 10:30	Morning Networking Break - Conservatory / Potsdam Foyer				
10:30 › 11:00	**Evaluating the Effectiveness of Fuzzy Hashing Techniques in Identifying Provenance of APT Binaries** Ms. Bhavna SOMAN (Intel Corporation)	**Protecting Privacy through Incident Response** Mr. Andrew CORMACK (Jisc)	**Building Community Playbooks for Malware Eradication** Mr. Christian SEIFERT (Microsoft)	Vulnerability Coordination - SIG	CERT Directory API - BoF - Chess
11:00 › 11:30	**Recent Trends of Android Malicious Apps: Detection And Incident Response in South Korea** Mr. Inseung YANG (KrCERT/CC), Ms. Jihwon SONG (KrCERT/CC)	**Defining and Measuring Capability Maturity for Security Monitoring Practices** Mr. Eric SZATMARY (Dell SecureWorks)	Building Community Playbooks for Malware Eradication (cont.)	Vulnerability Coordination - SIG (cont.)	CERT Directory API - BoF (cont.)
11:30 › 12:00	**A Study on the Categorization of Webshell** Mr. Jinwan PARK (KrCERT/CC)	**ENISA Threat Landscape: Current and Emerging Threat Assessment** Dr. Louis MARINOS (ENISA)	**A Cognitive Study to Discover How Expert Incident Responders Think** Mr. Sam J. PERL (CMU SEI CERT/CC)	Vulnerability Coordination - SIG (cont.)	
12:00 › 13:00	Lunch - LA Café & Pavillon				
13:00 › 14:00	**VRDX-SIG: Global Vulnerability Identification** Mr. Art MANION (CMU SEI CERT/CC), Mr. Takayuki UCHIYAMA (JPCERT/CC), Dr. Masato TERADA (Hitachi Incident Response Team)	**Effective Team Leadership and Process Improvement For Network Security Operators** Mr. Jeremy SPARKS (United States Air Force)	**Global Standards Unification - How EU NIS Platform, NIST and IETF Standards are Breaking Barriers for Information Sharing and Automated Action** Ms. Merike KAEO (Doubleshot Security)		**Who's worked on CSIRT and Cybersecurity Capacity Development in Africa? - BoF - Check** Mr. Jamie LORD (CERT/CC), Tracy BILLS (CERT/CC), Wassie GOUSHE (CERT/CC), Bill JONES (CERT/CC)
14:00 › 15:00	**Il Buono, il Brutto, il Cattivo: Tales from Industry** Mr. Rich BARGER (ThreatConnect Inc.), Mr. Andre LUDWIG (Novetta Solutions)	**Unifying Incident Response Teams Via Multilateral Cyber Exercise for Mitigating Cross Border Incidents: Malaysia CERT Case Study** Mrs. Sharifah Roziah MOHD KASSIM (MyCERT, CyberSecurity Malaysia)	**A Funny Thing Happened on the Way to OASIS: From Specifications to Standards** Tom MILLAR (US-CERT)	**IPv6 Security Hands-on** Mr. Frank HERBERG (SWITCH-CERT)	Who's worked on CSIRT and Cybersecurity Capacity Development in Africa? - BoF (cont.) ~Ending 14:30~
15:00 › 15:30	Afternoon Networking Break - Conservatory / Potsdam Foyer				
15:30 › 17:30	AGM (Members Only) - Potsdam I			IPv6 Security Hands-on (cont.)	

June **19th**, Friday

	POTSDAM I	POTSDAM III	BELLEVUE	OTHER MEETINGS
08:45 › 09:00	Opening Remarks - Potsdam I			
09:00 › 10:00	**Keynote Presentation: The cybercrime techniques, tactics and procedures (TTP) have evolved towards the mobile apps world - Potsdam I** Mr. Chema ALONSO (Telefonica/Eleven Paths)			Internet Architecture Board (IAB) and Internet Society (ISOC) workshop on Coordinating Attack Response at Internet Scale (CARIS)
10:00 › 10:15	Morning Networking Break - Conservatory / Potsdam Foyer			
10:00 › 10:15				IAB and ISOC Workshop (cont.)
10:15 › 11:15	**Building CERT Team and Responding Incidents in the Large Energy Company.** Mr. Miroslaw MAJ (Cybersecurity Foundation)	**Implementation of Machine Learning Methods for Improving Detection Accuracy on Intrusion Detection System (IDS)** Mr. Bisyron MASDUKI (Id-SIRTII), Mr. Muhammad SALAHUDDIEN (Id-SIRTII)	**Streamlined Incident Response from a Forensic Perspective** Matthew ROHRING (U.S. Department of Homeland Security / U.S. Computer Emergency Readiness Team)	IAB and ISOC Workshop (cont.)
11:15 › 11:45	**Sector Based Cyber Security Drills - Lessons Learnt** Mr. Malagoda Pathiranage DILEEPA LATHSARA (TechCERT)	**Keeping Eyes on Malicious Websites - "ChkDeface" Against Fraudulent Sites** Mr. Hiroshi KOBAYASHI (JPCERT/CC), Takayuki UCHIYAMA (JPCERT)	**Discovering Patterns of Activity in Unstructured Incident Reports at Large Scale** Dr. Bronwyn WOODS (CERT Program, SEI, CMU), THOMAS MILLAR (US-CERT), Mr. Sam J. PERL (CERT CC)	IAB and ISOC Workshop (cont.)
12:00 › 13:00	Closing Remarks - Potsdam I			
12:00 › 13:00				IAB and ISOC Workshop (cont.)
13:00 › 14:00	Lunch - LA Café & Pavillon			
13:00 › 14:00				IAB and ISOC Workshop (cont.)
14:00 › 18:00				IAB and ISOC Workshop (cont.)