

Program Agenda / #FIRSTCON25

Last Modified: June 18, 2025 12:01:00 UTC

Sunday, June 22nd

	SOCIAL ACTIVITY
09:00 – 17:00	Hackathon (Registration Required - See Abstract Below) - Located in the Treehouse
17:30 – 18:00	FIRST Newbie Session in Hall A1
18:00 – 20:00	Sunday Welcome Reception - 1st Floor Balcony




Monday, June 23rd

	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)	SOCIAL ACTIVITY
08:20 – 09:30	Conference Opening & Welcome Remarks TLP:CLEAR				
09:30 – 10:30	Monday Keynote Address: Unpacking the Human Factor: Navigating Individual, Socio-Technical, and Systemic Challenges in Incident Investigations Nina Sunde (Norwegian Police University College, NO) TLP:CLEAR				







	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)	SOCIAL ACTIVITY
10:30 – 11:00	Networking Break with Exhibits in Hall E				
11:00 – 11:35		The Evolving Cybersecurity Governance Landscape: Non-State Actors, the UN Framework and Critical Infrastructure  Serge Droz (FIRST / Swiss FDFA, CH) TLP: CLEAR	From Unstructured CTI Reports to Yara/SPL via LLMs   Aaron Kaplan (independent / EC-DIGIT-CSIRC, AT); Jürgen Brandl (BMI, AT); Chris Horsley (Cosive, AU) TLP: GREEN	From TTPs to Deception: Crafting Strategies   Diego Staino (BASE4 Security, AR); Federico Pacheco (BASE4 Security, ES) TLP: CLEAR	
11:45 – 12:20		Case: City of Helsinki Data Breach 2024  Matias Mesiä (NCSC-FI, FI) TLP: CLEAR	We All Want Validation (in our SecOps Detections)  John Stoner (Google Cloud, US) TLP: CLEAR	Breaking Down Barriers: Analyzing Active Directory Security Across Industries  Gary Sun, Vivian Teng (CyCraft Technology, TW) TLP: CLEAR	
12:20 – 14:00	Lunch Break in Hall E				
14:00 – 14:35		Building Towards #SquadGoals - Brick by Brick to a Unified Cyber Response Effort  Michael S (National Cyber Security Centre - United Kingdom, GB) TLP: GREEN	A Look at New ASNs  John Kristoff (Dataplane.org, US) TLP: CLEAR	Uncovering the Whispers of an APT Targeting Specific Industries in South Asia  Sathwik Ram Prakki, Subhajeet Singha (Quick Heal, IN) TLP: CLEAR	



	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)	SOCIAL ACTIVITY
14:45 – 15:20		Securing a Global Conglomerate: Mitsui & Co.'s Journey from Chaos to Control  Takahiro Okuhara (MITSUI & CO., LTD., JP) TLP:AMBER	Modern MISP  Konstantin Zangerle (KIT-CERT, DE) TLP:CLEAR	Where Did I Put My Keys? Preventing Data Leaks at Scale with Automation  Braxton Plaxco (Red Hat, US) TLP:GREEN	
15:20 – 15:50	Networking Break with Exhibits in Hall E				
16:00 – 17:15	FIRST AGM (Annual General Meeting)				
17:30 – 19:30					Sponsor Showcase & Networking Reception in Hall E

Tuesday, June 24th






	PLENARY (HALL A1)	FIRST CORE (B3 M5-6)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)
09:00 – 09:35		FIRST CORE Session Getting People to Listen to Your Alerts  Hadyn Green (Principal Communications Advisor – FIRST, NZ) TLP:CLEAR	From Zero to Prepared: Implementing a Weekly Incident Response Drill Program  Jeffrey Carpenter (Accuray, Inc., US) TLP:CLEAR	The Ontology for SOC Creation Assistance and Replication (OSCAR): A Community-Derived Tool for Developing SOC Capabilities  Justin Novak (Software Engineering Institute, US) TLP:CLEAR	Response via Prevention Engineering  Steve McKinney, Lauren Tam (Stripe, US) TLP:AMBER











	PLENARY (HALL A1)	FIRST CORE (B3 M5-6)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)
09:45 – 10:20		FIRST CORE Session Enhancing Trust within Africa CSIRT Communities Using the “Carrot and Stick” Principle Eric Akumiah (FIRST, GH) TLP:CLEAR	Incident Preparedness Takeaways from 5000 Exercise Participants Erlend Andreas Gjære (Secure Practice, NO) TLP:CLEAR	The Party Isn't Over: Uncovering Konfety's Novel "Evil Twin" Technique Lindsay Kaye, Gavin Reid (HUMAN Security, US) TLP:CLEAR	I Got 99 Problems But a Decryptor Ain't One: How to Save \$1.5 Million on Ransom Via Manual Recovery of Encrypted VMs Anton Kalinin (Principal Security Consultant at CSIS Security Group A/S, First member, DK) TLP:GREEN
10:20 – 10:50	Networking Break with Exhibits in Hall E				
10:45 – 11:20		FIRST CORE Panel Diversity Discussion Mona Østvang (FIRST, NO) 10:45 – 12:05	Pivoting To Resilience: Disruptive Incidents And How We Prepare For Them Tom Millar (CISA, US); Eireann Leverett (Killara Cyber, GB); Wendy Nather (None, US); Hendrik Adrian (LACERT, JP) TLP:CLEAR 10:45 – 12:05	Anti-Forensics - You are Doing it Wrong (Believe Me, I'm an IR Consultant) Stephan Berger (InfoGuard AG, CH) TLP:CLEAR	Why Be the King When You Can Be the Rogue Prince? Insights from Scraping of I2P and Freenet Lorenzo Nicolodi (Microlab.red, IT) TLP:AMBER
11:30 – 12:05				Aztronomy: Establishing the Foundation of Attack Path Analysis in Azure Tung-Lin Lee (Cycraft, TW) TLP:CLEAR	Routing Security for Enterprises: Secure Your Supply Chain Andrei Robachevsky (Global Cyber Alliance, NL) TLP:CLEAR
12:05 – 13:30	Lunch Break in Hall E				



	PLENARY (HALL A1)	FIRST CORE (B3 M5-6)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)
13:30 – 14:05		FIRST CORE Session Assessing CSIRT Maturity Across Africa's Regional Economic Communities: Implications for Capacity Building  Lawrence Muchilwa (FIRST, KE); Andy Chadwick (Shadowserver Foundation) TLP: CLEAR	Building the Blueprint: Designing Effective Storyboards for Cybersecurity Tabletop Exercises  John Hollenberger (Fortinet, US) TLP: CLEAR	It Wasn't Me - Sharing Threat Intel Anonymously using Abracadabra   Andras Iklody (CIRCL, LU); Trey Darley (Liaison, BE) TLP: CLEAR	Apollo Program : From Planet Earth to Space!  Jun Hyeong Lee (PLAINBIT, KR) TLP: AMBER











	PLENARY (HALL A1)	FIRST CORE (B3 M5-6)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)
14:15 – 14:50		FIRST CORE   Workshop Cyber Crisis Unplugged: Mastering Tabletop Exercises John Hollenberger (Fortinet, US); Douglas Santos (Fortinet, CA) TLP: CLEAR	Social Engineering in the Age of AI: Rethinking Security Awareness Training  Cornelia Puhze (SWITCH-CERT, CH) TLP: CLEAR	AWS Advanced Offensive Techniques, What Defenders Need to Know  Santiago Abastante (Solidarity Labs, AR) TLP: CLEAR	Persona Theory: Infiltration & Deception of Emerging Threat Groups  Tammy Harper (Flare, CA) TLP: AMBER
15:00 – 15:35		14:15 – 16:15 	RE(HACK)T: Open-Sourcing a Boardgame for User Awareness  Emilien Le Jamtel, Francien Giebels, Marton Szabo (CERT-EU, BE) TLP: CLEAR	Maximizing the Potential of AWS-WAF: Fully Automating threat detection with Custom Managed Rules and Proprietary Threat Intelligence  Shota Sugawara, Hirofumi Kawauchi (NTT-ME CORPORATION, JP) TLP: CLEAR	The Negotiation Paradox  Jan Kaastrup (CSIS Security Group, DK); Michael Sjøberg (Delta Crisis Management, DK) TLP: AMBER
15:35 – 16:05	Networking Break with Exhibits in Hall E				
16:05 – 17:05	Lightning Talks!				










Wednesday, June 25th

	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)	SOCIAL ACTIVITY
08:45 – 09:00	Wednesday Remarks TLP: CLEAR				



	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)	SOCIAL ACTIVITY
09:00 – 10:00	Wednesday  Keynote Address: TIIP - Threat Intel Informed Infrastructure Protection Søren Maigaard (SektorCERT, DK) TLP:AMBER				
10:00 – 10:30	Networking Break with Exhibits in Hall E				
10:30 – 11:05		Best Practices for Data Privacy Breach Response: Lessons Learned from Social Media Case Studies  Anne Connell, Lauren Cooper (Carnegie Mellon University, US) TLP:CLEAR	From p0f to JA4+: Network Fingerprinting and Reconnaissance  Vlad Iliushin (Cybersecurity Expert @ ELLIO, President of AMTSO (Anti-Malware Testing Standards Organization), CZ) TLP:GREEN	Inside the Information Stealer Ecosystem: From Compromise to Countermeasure  Olivier Bilodeau (Flare, CA) TLP:CLEAR	
11:15 – 11:50		Why is Finnish Healthcare Doing So Well Against Ransomware?  Perttu Halonen (National Cyber Security Centre Finland, FI) TLP:CLEAR	Beyond CVEs: Mastering the Landscape with Vulnerability-Lookup  Alexandre Dulaunoy (CIRCL, LU) TLP:CLEAR	Crypted Hearts: Exposing the HeartCrypt Operation   Daniel Bunce (Palo Alto Networks, Unit 42, DE); Jerome Tujague (Palo Alto Networks, Unit 42, US) TLP:GREEN	
11:50 – 13:15	Lunch Break in Hall E				



	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)	SOCIAL ACTIVITY
13:15 – 13:50		 Enhancing Incident Response with AWS CIRT, MSSPs, and ISVs Matthew Gurr (Full Membership via Amazon, AU); Lindsey Henry (US) TLP: CLEAR	 Evading in Plain Sight: How Adversaries Beat User-Mode Protection Engines Omri Misgav (Independent, IL) TLP: CLEAR	 From OSINT to Production Floor: How Threat Actors Can Infiltrate Your OT Operations Without You Even Knowing Claudiu Chelaru (Mnemonic, DK) TLP: CLEAR	
14:00 – 14:35		 Beyond Scanners and Tickets: A New Paradigm for Attack Surface Management Eirik Nordbø, Anders Nese (Equinor ASA, NO) TLP: GREEN	 The Dark Side of Digital Ads: How to Protect Your Brand using Meta AD Library Giuseppe Morici, Grazia Leonetti (Intesa Sanpaolo S.p.A., IT) TLP: AMBER	 Breaking the SIEM Confinement Anthony Talamantes, Todd Kight (Johns Hopkins University Applied Physics Laboratory, US) TLP: CLEAR	
14:45 – 15:20		 Bringing Actionable Data to Internet Defenders: Threat & Vulnerability Intelligence Capacity Building Efforts Across the Planet Piotr Kijewski (The Shadowserver Foundation, NL) TLP: CLEAR	 What Can Threat Intel Teams Learn from Journalists? Chris Horsley (Cosive, AU) TLP: CLEAR	 Broken Seals, Broken Trust: Flaws and Defences in the Certificate Ecosystem Yuta Sawabe, Rintaro Koike (NTT Security Holdings, JP) TLP: CLEAR	
19:00 – 22:00					Conference Social Event in Hall D3



Thursday, June 26th



	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)
09:00 – 09:35		Managing a CSIRT - Building Resilience and Fostering a Culture  Rick Logan-Stanford (TTCSIRT, TT); Joyce Isa-Molwane (Botswana Communications Regulatory Authority, BW) TLP:GREEN	The Funny Story of Active Directory Backdooring  Sylvain Cortes (Hackuity, FR) TLP:CLEAR	Detection Engineering 101 : Establishing a Structured Approach to Detection Engineering  Tomohisa Ishikawa (Tokio Marine Holdings, JP) TLP:CLEAR
09:45 – 10:20		TLP:GREEN 09:00 – 10:00	Guardians of the Hypervisor  Nicklas Keijser (Truesec CSIRT – Truesec, SE); Anders Olsson (Truesec, SE) TLP:CLEAR	Navigating the Threat Actor Maze: A Tool for Mapping Names, Families and Insights  Dave Matthews (Avast (Gen Digital), AU) TLP:CLEAR
10:20 – 10:50	SIG Updates 10:20 – 11:20	Networking Break with Exhibits TLP:CLEAR Networking Break with Exhibits in Hall E 10:20 – 11:20		
10:45 – 11:20		Engaging with the Media to Foster Cybersecurity Resilience  Zivile Necejauskaite (NRD Cyber Security, LT); Madara Krutova (Latvia's CERT.LV, part of the National Cybersecurity Centre, LV) TLP:CLEAR	Versus Killnet  Alex Holden (Hold Security LLC, US) TLP:CLEAR	Understand and Detect - Stealthy Techniques Used to Conceal Artifacts on Modern Linux Systems  Robert Byrne (Ericsson, AU) TLP:GREEN








	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)
11:30 – 12:05		All Ransomware Economic Models are Wrong, But This One is Useful  Eireann Leverett (Killara Cyber, GB) TLP:CLEAR	Lazarus Group Evolved Their Infection Chain with Old and New Malware  Sojun Ryu (Kaspersky, KR) TLP:CLEAR	A Story about Fighting Disinformation or How We Helped the Russian Trolls  Krassimir Tzvetanov, PhD (Purdue University, US) TLP:GREEN
12:05 – 13:30	Lunch Break in Hall E			
13:30 – 14:05		Burnout: Detect, Investigate, Respond, Recover, Prevent   Désirée Sacher (Finanz Informatik, DE); Carson Zimmerman (Microsoft, US) TLP:CLEAR	Threat Hunting with Python & Pandas  Anthony Talamantes, Matt Dulle (Johns Hopkins University Applied Physics Laboratory, US) TLP:CLEAR	Revolutionizing Malware Analysis with Agentic AI: Lessons and Innovations  Justin Page (Booz Allen Hamilton, US) TLP:CLEAR
14:15 – 14:50		Unmasking Cyber Security: Rethinking Small to Medium Business Security Awareness  Sophie Horgan (NCSC, NZ) TLP:CLEAR	Artemis: How CERT PL Improves the Security of the Polish Internet  Krzysztof Zając (CERT PL, PL) TLP:CLEAR	Using DNS Registry and Requests for Securing .pl TLD and Beyond  Piotr Białczak, Paweł Pawliński (CERT.PL/NASK, PL) TLP:GREEN
15:00 – 15:35		Developing a Sectoral CERT Ecosystem  Albert Antwi-Boasiako, Stephen Cudjoe-Seshie (Cyber Security Authority, GH) TLP:GREEN	The Convergence of Threat Behaviors Across Intrusions  Joe Slowik (The MITRE Corporation, US) TLP:CLEAR	Keypocalypse  Emilien Le Jamtel (CERT-EU, BE) TLP:GREEN
15:45 – 16:15	Networking Break with Exhibits in Hall E			
16:15 – 17:15	Lightning Talks!			



Friday, June 27th

	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)
09:00 – 09:35		What Can Cybersecurity Incident Responders Learn from Real-World Crises?  Matt Palmer (Jersey Cyber Security Centre, JE) TLP:CLEAR	Automated ATT&CK Technique Chaining  Martin Eian (mnemonic, NO) TLP:CLEAR	Forecasting Cybersecurity Data: Making Sense of the Senseless  Vijay Sarvepalli (US) TLP:CLEAR
09:45 – 10:20		One SOC, The Whole SOC, and Nothing But The SOC, So Help Me  Carson Zimmerman (Microsoft, US) TLP:CLEAR	What's New in CSAF v2.1: Key Updates Explained   Justin Murphy (DHS/CISA, US); Thomas Schmidt (BSI, DE) TLP:CLEAR	Unmasking MSC Files: A Deep Dive into APT Weaponization, Grim Resource Injection, and AppDomain Manager Hijacking  Hossein Jazi, Douglas Santos (Fortinet, CA) TLP:CLEAR
10:30 – 11:05		PSIRT 2.0: Revolutionizing Product Security with the Generative AI Strategy - Approach for Empowering Product Cyber Resilience and PSIRT Operation   Hikohiro Lin, Kosuke Ito (GMO Cybersecurity by IERAE, Inc., JP); Ken Lee (Independent Security Advisor, TW) TLP:AMBER	Only Seeing Stars: Enabling the Open Source Scripting Community with OCSF  Michael Bunner (REI, US) TLP:CLEAR	Establishing a Global Community of Practice on Coordinated Vulnerability Disclosure (CVD)   Tomo Ito (JPCERT Coordination Center, JP); Justin Murphy (DHS/CISA, US) TLP:CLEAR



	PLENARY (HALL A1)	TRACK 1 (AUDITORIUM 10)	TRACK 2 (AUDITORIUM 11)	TRACK 3 (AUDITORIUM 12)
11:15 – 11:50		Behind the Mask  Denys Yashchuk (CERT-UA, UA) TLP:GREEN	99 Bottles of Trust on the Wall: Approaches to Building Convivial Communities   Trey Darley (Liaison, BE); Tom Millar (CISA, US) TLP:CLEAR	Comprehensive Investigation Results on Malware Code Interpretation by GPT-4  Yasuyuki Tanaka (NTT Social Informatics Laboratories, JP) TLP:CLEAR
11:50 – 12:20	Networking Break in Hall E			
12:20 – 13:20	Friday Keynote Address - Network Security is a Team Sport, so How Do We Set and Manage the Team  Christian Damsgaard Jensen (Aarhus University, DK) TLP:CLEAR			
13:20 – 13:50	Closing Remarks TLP:CLEAR			
13:50 – 14:50	Lunch Break in Hall E			