Issued on Nov. 13 , 2026

Day1 Tue, Nov. 17

Track1 (HALL B)

Time	Category, Keywords	Title	Speaker	Lang.
09:00 - 09:55	Keynote (AI, International Law & Policy, Education)	Cybersecurity and Capacity Building in the Frontier AI Era (tentative)	Christian Van Heurck Ioannis Agrafiotis	EN
10:10 - 10:50	Techical (AI, Web App Security, Bug Bounty)	[Pwn2Own Berlin 2026 $20,000] Agent2Shell: Your AI Coding Agent Already Ran the Attacker's Code	Satoki Tsuji	JA
11:00 - 11:40	Technical (AI, Bug Bounty, Cyber Crimes)	AI vs. AI: AI-Assisted Research into a Privilege Escalation Bug in the Google Pixel AI Coprocessor	Poh Kang Yu	EN
11:50 - 12:30	Technical (AI)	ChatMate: Remote Prompt Execution on AI Assistants through Sandbox Escaping	Ori Lahav	EN
13:40 - 14:20	Technical (AI)	The Evolution of Adversarial AI: Tales from the Frontlines of Threat Intelligence	Daniel Kapellmann Zafra	EN
14:30 - 15:10	General (AI, Bug Bounty)	Pwning Agentic Browsers with PleaseFix: A New Vulnerability Class for 0-Click Takeover	Stav Cohen Michael Bargury	EN
15:30 - 16:10	General (AI, Digital Forensics)	Quality Assurance for Incident Response in the Age of AI	Shusei Tomonaga Yuki Yano	JA
16:20 - 17:00	Techical (AI, Web App Security, Bug Bounty)	In Origin We Trust: Breaking Chromium from Its Privileged Side	Orange Tsai	EN
17:10 - 17:50	Techical (Critical Infrastructure, Authentication)	Pass-the-Device: Transplanting SASE/VPN Trust After Endpoint Compromise	Ruslan Sayfiev	JA
18:00 - 18:40	Counter Cyber Crime (Cyber Crimes, Ecucation)	From the Rebellious Cities: How Iranian APTs spy on their own people	Eliad Kimhy Subhajeet Singha	EN

● Track2（HALL A）

Time	Category	Sponsor, Title	Speaker	Lang.
10:00 – 10:30	Open Talks	[Mitsui Bussan Secure Directions, Inc.] Threat Trends in AI Agents and Multi-Layered Defense with Secure AI Gateway	Isao Takaesu Shohei Koda	JA
10:40 – 11:10	Open Talks	[OffSec] Cheap Exploits, Scarce Judgement: Human Resilience in Japan's Active Cyber Defense Era	Tim Norman	EN
11:20 – 12:05	Open Talks	[Hitachi Systems, Ltd.] Part 1: Why Frontier AI Is Rewriting Cyber Warfare: Preparing for AI That Can Serve as Both Sword and Shield Part 2: China's Military Use of Artificial Intelligence	Part 1: Hirofumi Nakakoji Part 2: Bonji Ohara (Senior Fellow Sasakawa Peace Foundation)	JA
13:00 – 13:45	Open Talks	[Panasonic Holdings Corporation] How to Work with Threat Intelligence	Manabu Nakano	JA
13:55 – 14:40	Open Talks	[GMO Internet Group] Behind Endless Vulnerability Headlines, Malicious Packages Keep Coming: Software Supply Chain Attacks Seen Through 19 Million Package Versions	Keijiro Toyoda	JA
15:00 – 15:30	Open Talks	[SCSK Security Corporation] Navigating Frontier AI Risks and Governance: Lessons from Japan and Global Standards	Shigenori Takei	JA
15:40 – 16:10	Open Talks	[Macnica, Inc.] Unknown Assets, No Time to Wait for KEV: What ASM and Risk-Based Vulnerability Management Can—and Can't—Do in the AI Era	Takeya Yamazaki Yudai Yahara	JA
16:20 – 16:50	Open Talks	[NRI SecureTechnologies, Ltd.] Toward an Agentic SOC That Surpasses Expert Analysts: Organizational Knowledge Injection and Harness-Based Control	Yumehisa Haga	JA

● Track3（Room3）

Time	Category, Keywords	Title	Speaker	Lang.
12:00 – 12:40	Bluebox (AI)	Antigent: An Autonomous Counter-Agent Against Agentic AI Attacker	Hiroaki Toyota	JA
13:00 – 13:40	Bluebox (AI)	One Harness, Three Security Agents: Recursive Language Models in Practice	Syue Siang Su	EN
14:00 – 14:40	Bluebox (AI)	Turncoat: From Coding Agent to C2 Agent	Michael Telloyan	EN
15:00 – 15:40	Bluebox (AI)	vwhois: A Practical WHOIS Parser Conquering the Wilderness of All TLDs	Hiroki Hada	JA
16:00 – 16:40	Bluebox (AI)	Static Analysis for AI Applications: From Taint Tracking to Exploit Generation	Alisha Gupta	EN
17:00 – 17:40	Bluebox (AI, Data Protection, Authentication)	AgentShield: Stopping a Rogue AI Agent in the Linux Kernel	Weixiao JI Qingzhe Jiang Leandro Li	EN

Day2 Wed, Nov.18

Track1 (HALL B)

Time	Category, Keywords	Title	Speaker	Lang.
09:00 – 09:40	Technical (Malware Countermeasure)	Shade Core: Bringing UEFI Attacks Back to Hypervisor-Protected Modern PCs	Kazuki Matsuo	JA
09:50 – 10:30	Technical (Bug Bounty)	Vulnerabilities Assembled! The Cross-Component Vulnerability Factory Inside the Windows Kernel	Angelboy Yang	EN
10:40 – 11:20	Counter Cyber Crime (AI, Malware Countermeasure, Digital Forensics)	Five Years of GitHub Monitoring: Unveiling the Lifecycle of Malicious and For-Sale PoCs	Ryosuke Yoshimura	JA
11:30 – 12:10	Counter Cyber Crime (Malware Countermeasure, Digital Forensics)	Operation ShadowCommit - Hidden Ops on Github	Jun Hyeong Lee Daehoo Lee	EN
13:20 – 14:00	Technical (AI, Critical Infrastructure, Hardware Hacking)	Too Close to the Metal: Attacking GPU Neo-Clouds from the Inside and Out	Michael Katchinskiy Yakir Kadkoda	EN
14:10 – 14:50	Law & Policy (Critical Infrastructure)	The Code IS the Law: Private Norm-Making in the Cybersecurity Governance of Outer Space	Joanna Kulesza	EN
15:00 – 15:40	Law & Policy (Critical Infrastructure)	Salt Typhoon's Shadow: Japan and the Staging Grounds Next Door	Christopher Braccia	EN
15:50 – 16:30	General (Critical Infrastructure, Cyber Crimes)	Countering Physical-to-Cyber Attack: Physical Intrusion of Major Plants and Business Risk Assessment using CPSF	Daisuke Ota	JA
16:40 – 17:20	General (OT, IoT Security, Critcal infurastructure)	When the Spectrum Becomes the Battlefield: Defending Municipal IoT Under Jamming	Pavlo Chernikov	EN
17:30 – 18:10	General (Critical Infrastracture, Malware Countermesuare)	Defending Critical National Infrastructure in a Hybrid Threat Landscape	Ivan Kalabashkin	EN

● Track2 (HALL A)

Time	Category, Keywords	Sponsor, Title	Speaker	Lang.
09:00 – 09:40	U25 (Web App Security)	No Context, No Consent: A Systematic Analysis of LNA Bypasses in Firefox's Internal Request Paths	Rintaro Kawasugi	EN
09:50 – 10:30	U25 (Bug Bounty)	Out of LINE： QR Code to Wormable RCE in LINE Client	Lin Hong-Teng	EN
10:50 – 11:20	Open Talks	[SSD Labs Japan] MIBleed: An 11-Year-Old Bug Every Tool Missed	Aaron Cho	EN
11:30 – 12:00	Open Talks	[NTT DATA INTELLILINK Corporation] Vulnerability Management in the Frontier AI Era: Closing the Gap Between Attackers and Defenders	Shigeki Yabune	JA
13:00 – 13:30	Open Talks	[MS&AD InterRisk Research & Consulting, Inc.] After a Cyber Incident: What Every Company Must Do Next — Guidance from Legal Experts	Shunsuke Terakado (TMI Associates, Partner) Noritaka Endou Jun Matsumori	JA
13:40 – 14:10	Open Talks	[NTT Security (Japan)] Attribution of Threat Actors Using OSINT 2026	Taro Manabe	JA
14:20 – 14:50	Open Talks	[NEC Corporation] Hunting C2 Infrastructure from Abused ManageEngine Servers: Tracing and Analyzing ValleyRAT and AtlasRAT	Hiroshi Oshiba Takaaki Sugiu Daisuke Maeda	JA
15:00 – 15:30	Open Talks	[HireRoo, Inc.] What 1.18 Million Real-World Data Points Reveal: Safety and Guardrail Design for AI Agents in Organizations	Kosuke Kuzuoka	JA