Post event report

e-Crime & Cybersecurity Switzerland

17th September 2026, Zurich

Principal Sponsor

Strategic Sponsors

Education Seminar Sponsors

Networking Sponsor

Branding Sponsor

Inside this report:

Key themes

AI and quantum

- Identity, authority, and control for non-human actors
- Data protection and leakage risks
- AI anti-phishing and social engineering defences
- Who needs to be quantum-ready?
- Integrity and the AI-enabled supply chain
- Intelligent Threat Detection

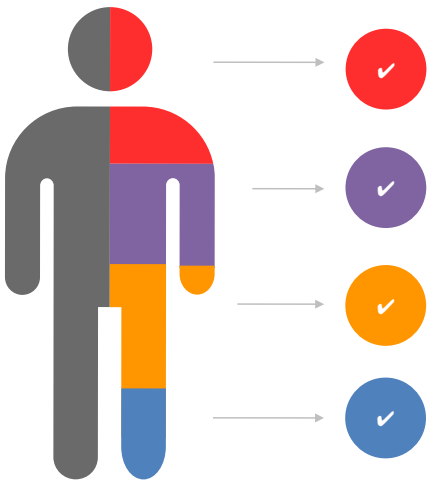
Building better security

- Making the best use of threat intelligence
- Security posture management
- Improving continuous attack surface discovery
- The power of automation
- Adversary simulation and behavioural analysis
- Securing the Cloud: still a problem

Best practice fundamentals

- Achieving visibility across ecosystems
- Transitioning OT to the Cloud?
- Defending against the latest ransomware variants
- Securing the basics
- Why zero trust, isolation and segmentation are key
- Dealing with regulations

Who attended?



Cyber-security
We have a 15-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Gary Adams, Sales Engineer Leader, **Rubrik**

Andrea Arquint, Principal Solutions Engineer, **F5**

Simon Brady, Event Chairman, **AKJ Associates**

Federico Casano, CISO, **YAPEAL**

Will Collison, Technical Director – Cryptography, **HSBC**

Dr. Diana Coman Schmid, CISO, **Canton of Glarus**

Andy Giles, Executive Director, Cyber & Technology Risk Reporting and Metrics, **JPMorgan Chase**

Chris Girling, Partner, Cybersecurity & Privacy, **PwC Switzerland**

Christian Götz, Director SE Programs, **Palo Alto Networks**

Philipp Grabher, CISO, **Canton Zurich**

Klaus Haller, Senior IT Security Architect, **AXA**

Alex Hitchen, Sales Engineer, **Huntress**

Ash Hunt, VP of Strategy, **Cyera**

Tom Kretzschmar, Sr. Sales Engineer, **Proofpoint**

Idir Laurent Khiar, DPO and AI Officer, Baltic Cluster, **Geopost SA**

Andreas Muller, Regional Sales Director CEUR, **Delinea**

Fidel Nozal, Account Executive, **ThreatLocker**

Antti Partanen, VP Security and CISO, **Sunrise**

Johanna Peterson, Senior Manager, Cyber, Crisis and Resilience, **PwC Switzerland**

Juan Carlos Lopez Ruggiero, Lecturer, **HSLU, Lucerne**

Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, **Bank of England**

Dustin Schwinning, Senior Sales Executive, **Open Systems**

Jan Schulze, Manager, Cybersecurity, Resilience and Defence, **PwC Switzerland**

Jonathan Sinclair, Head of Cyber Resilience PT, **Roche**

Agnès Terreau, Country DPO & Security Officer, **ManPower Group**

Agenda

08:00 Breakfast networking and registration

08:50 Chairman's welcome

09:00 **Ready to recover: The true test of cyber-resilience**

Andy Giles, Executive Director, Cyber & Technology Risk Reporting and Metrics, JPMorgan Chase

- How the threat has changed – the rise of state-based and hybrid cyber-activity, and the deteriorating threat environment
- Prepare to fail – why resilience incidents are not hypothetical but inevitable, and why readiness must be cultural, not procedural
- Match fit for recovery – what it means to be ready for data and systems restoration under real-world conditions
- Knowing when 'good enough' is good enough – how to measure resilience in ways that are predictive, embedded, and aligned with risk appetite

09:20 **The 3 AM test – why security outcomes are decided by the operating model rather than the tool stack**

Dustin Schwinning, Senior Sales Executive, Open Systems

- What is actually true about your controls at three in the morning on a Sunday
- Run versus Reduce – the one ratio that predicts your next budget round, how to measure it from your own ticket data, and how to frame it so the board funds it
- Four operating models, four failure modes – an honest comparison of in-house, self-run platform, managed wrapper and native managed, including where each one breaks and what it costs
- Where incidents actually get long – the four handoffs that consume most of your MTTR, and why counting them in your own post-incident reviews changes the conversation
- Six questions for your next RFP – practical wording to separate an operating model from a support contract, to be asked of every supplier, including Open Systems

09:40 **Two sides of the table: What two former practitioners see coming for enterprise data**

Chris Girling, Partner, Cybersecurity & Privacy, PwC Switzerland & **Ash Hunt,** VP of Strategy, Cyera

- Two speakers who ran security inside large enterprises before moving to advisory and product roles – why they made the move, and what it revealed about how enterprise environments are really changing
- Finding the sensitive data: The best approaches they have seen work at genuine enterprise scale, including lessons from a major financial services programme, and the ones that quietly fail
- Refactoring the enterprise: How control architecture is being rebuilt, what that does to legacy processes, and where the platform consolidation is heading
- AI threats and risks: What is new, what is recycled, and what practitioners should be doing about it now rather than in two years

10:00 **Real-world tactics for addressing AI security risks: Actions you can implement now**

Klaus Haller, Senior IT Security Architect, AXA

- Cutting through the noise: Industry hype and vendor fear-mongering versus AI security threats demanding genuine action
- Targeted risk assessment: Exploring the various AI types and the unique security vulnerabilities they introduce
- Practical defences & future challenges: Uncovering effective mitigation strategies and identifying AI security risks the industry is still learning to tackle

10:20 **Education Seminars | Session 1**

Open Systems **What operating model are you actually running?** **A working session** **Dustin Schwinning,** Senior Sales Executive, Open Systems	**Palo Alto Networks** **From identity silos to security at scale** **Christian Götz,** Director SE Programs, Palo Alto Networks

11:00 Networking break

Agenda

11:30 — **Quantum is coming. Financial services can't afford to wait**

Will Collison, Technical Director – Cryptography, HSBC

- Discover why the quantum threat to today's cryptography is closer and more disruptive than many realise
- Hear what's at stake for financial services as quantum computing reshapes the cybersecurity landscape
- Join the call for industry-wide collaboration to tackle one of cybersecurity's biggest ever challenges before the clock runs out
- Learn what you can do today (or already should be doing) to reduce your risk

11:50 — **Resilience for everything: How to ensure business continuity across cloud, identity, and AI**

Gary Adams, Sales Engineer Leader, Rubrik

- Ensure recoverable backups for on-premises, cloud, and SaaS data
- Protect, analyse, and restore identity systems – from AD to Entra ID and Okta
- Accelerate AI transformation while maintaining control and rolling back when necessary

12:10 — **Cybercrime unmasked: How hackers make money (and how to stop them)**

Alex Hitchen, Sales Engineer, Huntress

- Alex Hitchen goes undercover into the modern cybercrime economy, pulling back the curtain on how attackers really operate, and how you can shut them down before they cash out
- You'll follow the money trail from that first 'harmless' phishing email through Business Email Compromise (BEC), session token theft and Ransomware-as-a-Service
- Along the way, Alex will decode the roles of initial access brokers, affiliates and ransomware operators
- This will include how the same playbooks that fuel their profits can be used against them with the right visibility and response

12:30 — **AI on both sides: How attackers scale, defenders see, and enterprises stay in control**

Tom Kretzschmar, Sr. Sales Engineer, Proofpoint

- AI in the hands of attackers – what Proofpoint is seeing in the threat landscape today, where AI is genuinely changing attacks, and where the hype still exceeds reality
- Seeing threats at global scale – how worldwide threat telemetry and intelligence turn billions of signals into early detection, connecting attacker infrastructure, identities, communications and campaigns
- Securing AI inside the enterprise – how organisations can discover which AI tools and agents are being used, understand what data they access, and apply controls without standing in the way of adoption

12:50 — **Zero Trust controls at the endpoint**

Fidel Nozal, Account Executive, ThreatLocker

- Discover how ThreatLocker applies Zero Trust at the endpoint, eliminating implicit trust by continuously verifying every application, executable, and action before authorisation
- Learn how a deny-by-default, malware-proofing approach reduces ransomware risk, stopping unauthorised software and scripts even when other security layers are bypassed
- Understand how least-privilege enforcement limits attacker capability, ensuring applications and users can perform only explicitly approved actions on enterprise devices
- Explore how granular, policy-based endpoint control safeguards against modern threats, reducing enterprise exposure to ransomware and other advanced attacks

12:55 — Lunch and networking

14:00 — **PANEL DISCUSSION** **Beyond compliance – building cyber-resilience that actually works**

Simon Brady, Event Chairman (Moderator);
Jonathan Sinclair, Head of Cyber Resilience PT, Roche;
Philipp Grabher, CISO, Canton Zurich;
Juan Carlos Lopez Ruggiero, Lecturer, HSLU, Lucerne

- How do we turn risk appetite statements into real decision levers instead of paperwork?
- With NIS2 and similar rules, what does 'appropriate and proportionate' really mean on the ground – and how can risk management steer the response?
- Which cyber-metrics really matter – and how do we prove our risk posture to the Board, to clients, and across the entire supply chain, right down to nth-party dependencies?
- How does a resilience-first mindset transform culture – moving from blame and unrealistic prevention to readiness, adaptability, and fast recovery?

Agenda

14:30 — **The AI was granted access. No one saw what it did next**

Andreas Muller, Regional Sales Director CEUR, Delinea

- Ensuring the use of AI creates genuine value rather than just risks
- Why authorisation alone isn't enough for agentic AI – and how Delinea StrongDM makes activity on critical systems visible in real time and controllable throughout the entire interaction
- Effective protection against ambiguous prompts or unwanted activities by both internal and third-party AI

14:50 — **Defining your Minimum Viable Company: Lessons from cyber-response**

Johanna Peterson, Senior Manager, Cyber, Crisis and Resilience, &
Jan Schulze, Manager, Cybersecurity, Resilience and Defence, PwC Switzerland

- Discover how organisations are unlocking the power of the Minimum Viable Company (MVC) to drive their resilience programmes: the critical products, services, and capabilities necessary to protect customers, revenue, and compliance during disruption
- Learn real-world, hard-won lessons from cyber-response that highlight the value of identifying your MVC before an attack, enabling faster and more effective recovery
- Hear the no-regret actions and practical steps to engage your organisation on MVC, turning resilience planning into a shared organisational priority

15:10 — **Education Seminars | Session 2**

F5
Securing the AI workload: Defending enterprise LLMs and agentic systems
Andrea Arquint, Principal Solutions Engineer, F5

15:40 — Networking break

16:00 — **PANEL DISCUSSION** **The corporate security case for AI sovereignty**

Simon Brady, Event Chairman (Moderator); Federico Casano, CISO, YAPEAL;
Idir Laurent Khiar, DPO and AI Officer, Baltic Cluster, Geopost SA;
Agnès Terreau, Country DPO & Security Officer, ManPower Group;
Dr. Diana Coman Schmid, CISO, Canton of Glarus; Antti Partanen, VP Security and CISO, Sunrise

- Your AI runs on someone else's infrastructure, under someone else's law – is that a security risk your board has signed off on?
- Do you actually know which AI models are running inside your organisation – and do you control what data they see and send out?
- NIS2, the AI Act, and GDPR each touch AI sovereignty differently – how do you build one coherent security programme when the regulations pull in different directions?
- If your primary AI vendor became inaccessible tomorrow – through outage, sanctions, or a geopolitical event – how long before your operations fail, and do you have a continuity plan?

16:30 — **Invisible leaks: The hidden risks of chatting with AI**

Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England

- AI privacy risks: How tools like ChatGPT, Claude, and Co-Pilot can end up knowing more about you than your best friend (and never forget a thing). The hidden dangers of casually sharing information with AI
- When small details add up: Why a few 'harmless' details can combine to paint a full picture & how scattered information can reveal sensitive data without you realising
- The myth of security: Why AI models aren't as secure as we might think & how attackers can trick them into spilling information
- Simple, practical steps: For employees: how to keep personal and company data safe & For organisations: reducing AI-related risks before they grow

16:50 — Chairman's closing remarks

17:00 — Drinks reception & networking, kindly Sponsored by PwC Switzerland

18:00 — End of conference

Education Seminars	
F5 **Securing the AI workload: Defending enterprise LLMs and agentic systems** **Andrea Arquint,** Principal Solutions Engineer, F5	As enterprises move Generative AI and LLMs into production, security teams face a paradigm shift. Securing AI is no longer just about defending against 'AI-powered attackers' (AI as a Weapon); it is fundamentally about safeguarding the AI infrastructure itself (AI as a Workload). This session explores the unique security challenges of integrating LLMs into corporate environments. We will focus on critical threat vectors like prompt injection, sensitive data leakage via RAG pipelines, and the governance risks of autonomous agentic systems. As an F5 Principal Solutions Engineer, Andrea Arquint will deliver a practical corporate defence blueprint using the F5 AI Security & Delivery Platform (ADSP). **Attendees will learn:** • How to enforce real-time In-Line AI Guardrails to sanitise prompts and prevent outbound data leakage • How to leverage Continuous Agentic Red Teaming for proactive model benchmarking and auto-remediation • How to secure LLM APIs and manage token consumption at the network ingestion layer • How to gain the strategic framework and technical insights needed to confidently secure your enterprise AI adoption.
Open Systems **What operating model are you actually running? A working session** **Dustin Schwinning,** Senior Sales Executive, Open Systems	Most security programmes are well tooled and poorly operated. The controls are bought, deployed and documented – but who runs them, at what level of skill, and at what hour is often the last question asked and the first one that matters when something breaks. This working session is not a presentation. Participants score their own environment against the factors that genuinely determine which operating model fits: the number of handoffs between separate owners, the out-of-hours coverage the business actually requires, change frequency, jurisdictional exposure, and the realistic availability of Level-3 skills. Company size is one input among these, not the answer. Positions are then compared live across the room, and each outcome is stress-tested against the failure mode it carries. The session is deliberately open-ended: for some organisations the right answer is to keep operations in-house and change how they are measured; for others it is to change the contract rather than the supplier. **Attendees will learn:** • A repeatable way to determine which operating model fits their constraints, independent of vendor or company size • A method for measuring their own Run-versus-Reduce ratio from existing change and incident data • The failure mode of each operating model, including the one Open Systems operates, and how to contract against it • Six questions to put to any supplier – including this one – that separate an operating model from a support contract

Education Seminars	
Palo Alto Networks **From identity silos to security at scale** **Christian Götz,** Director SE Programs, Palo Alto Networks	As identities, cloud resources, machine identities and AI agents become increasingly interconnected, traditional, fragmented approaches to identity security are no longer enough. In this session, Palo Alto Networks Idira explore how organisations can move beyond security silos toward a unified, scalable approach that improves visibility, reduces risk, and enables secure business agility. **Attendees will learn:** • How persistent access privileges increase the modern enterprise attack surface • Why a unified approach is needed to manage human, machine, cloud, and AI identities • How Zero Standing Privilege (ZSP) can reduce risk by granting privileged access only when it is needed • Practical principles for breaking down identity security silos while maintaining agility and productivity