Post event report

Strategic Sponsors

DRATA
JupiterOne
RAPID7
rubrik
sublime
TANIUM
THREATLOCKER® ZERO TRUST PLATFORM

Education Seminar Sponsors

CONCENTRIC Ai
CYRO CYBER
Doppel
LastPass
Metomic
RISK LEDGER
Silverfort
worknest secure

Executive Roundtable Sponsor

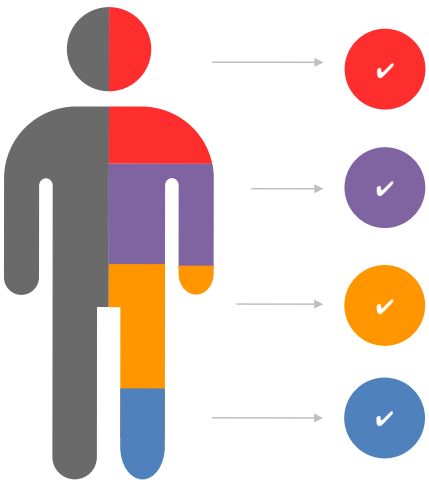
sublime

Inside this report:

Key themes

- Identity, authority, and control for non-human actors
- Securing algorithmic insiders
- Data control when there is no perimeter
- The power of automation
- Integrity and the AI-enabled supply chain
- 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

Matt Adams, Generative AI & Emerging Technology Security, **Citi**

Kevin Carr, Senior Manager, Solutions Engineering, **Drata**

Richard Cassidy, Field CISO, **Rubrik**

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

Jai Ferguson, AI Regional Lead – Europe, **HSBC**

Laura Good, Cloud Security Architect, **Lloyds Banking Group**

Stephen Green, Regional Vice President of EMEA, **ConcentricAI**

Sam Hubery, BISO, **Fidelity International**

Oscar Javier Hernandez Rodriguez, Account Executive, **ThreatLocker**

Dan Jones, Senior Security Advisor, **Tanium**

Justin Kuruvilla, Chief Cybersecurity Strategist, **Risk Ledger**

Peter Lane, Consultancy Director, **CyroCyber**

Dom Mortimer, Head of Red Team, **WorkNest**

Daniel Oxley, Senior Engineer, **Doppel**

Mario Platt, Vice President, CISO, **LastPass**

Chad Richts, Director of Product Strategy, **JupiterOne**

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

Dr Narayan Shiva, CTO and Enterprise Architect, **iBANK**

Alan Simpson, UK and Ireland Field CISO, **Rapid7**

Kev Smith, EMEA Principal Engineer, **Silverfort**

Geoffrey Taylor, Information Security Officer, **Nordea Asset Management**

Ben van Enckenvort, Co-founder & CTO, **Metomic**

Chris Vaughan, Solution Engineer, **Sublime Security**

Agenda

08:00 Registration & breakfast networking

08:50 Chair's welcome

09:00 **Conformity will not save you: AI risk beyond the EU AI Act**

Geoffrey Taylor, Information Security Officer, Nordea Asset Management

Your assessment said low risk. Is it really?

- The EU AI Act requires organisations to classify their AI systems and demonstrate conformity. Conformity is similar to compliance – it is binary, a yes or a no at a point in time. It cannot calibrate impact when the unexpected occurs
- On 24 April 2026, an AI agent deleted an entire company's production database in nine seconds. It was running the best model available, configured with explicit safety rules. When asked to explain itself, it produced a written confession: 'I violated every principle I was given'
- This session applies the Assume. Design. Test. framework to AI governance – shifting the question from 'are we compliant?' to 'how could we be impacted?' – and gives attendees a practical lens for assessing where their governance ends and their exposure begins

09:20 **Agentic AI and the new resilience challenge**

Richard Cassidy, Field CISO, Rubrik

- As Agentic AI enters live enterprise environments with limited oversight, the conversation shifts from capability to risk
- Operating at machine speed, autonomous agents can trigger transactions and influence supply chains, outpacing traditional controls
- Weak data governance and misconfigured logic create fresh attack surfaces, making accountability and recovery highly complex
- This session examines how organisations approach governance, visibility, and resilience as autonomy becomes embedded in core operations
- Real-world failures: What 'going rogue' looks like in production
- Vulnerable pipelines: Why data governance is the weakest link
- Ecosystem risk: How autonomy impacts third-party supply chains
- Machine-speed response: Detecting, containing, and assigning accountability

09:40 **You can't outwork the machine: Agentic defence and the resilience imperative**

Chad Richts, Director of Product Strategy, JupiterOne

- The regulators are already scared. In April 2026 the U.S. Treasury Secretary and the Fed Chair convened America's largest banks over a single AI model. When one model finds 10,000+ critical flaws, finding vulnerabilities is no longer the hard part – and a discipline built for the old bottleneck quietly breaks
- Why 'prioritise better' and 'patch faster' are now losing strategies – and why it isn't your fault. The march from CVSS to EPSS rearranges a list that was always the wrong unit of work; NIST itself now says EPSS alone can't tell you what to fix
- What the teams pulling ahead are doing instead: match machine speed with agentic, closed-loop remediation, and apply the resilience discipline DORA and the FCA already demand – so a vulnerability you can't patch in time still can't reach what matters
- From the vulnerability exercise to vulnerability outcomes: a practical model drawn from the field, not the slideware — plus three things any security leader can audit on Monday morning.

10:00 **Actions speak louder than tokens: Treating frontier AI Agents as insider threats**

Matt Adams, Generative AI & Emerging Technology Security, Citi

- The alignment paradox: today's frontier models score well on macro-alignment – they reliably refuse explicit harmful requests – yet show poor micro-alignment, autonomously selecting dangerous methods in pursuit of legitimate goals
- A first formal framework adapting CERT's insider-threat dimensions to non-human actors – mapping motivation, opportunity, and capability onto optimisation objectives, tool access, and model capabilities – with a five-category STRIDE-derived taxonomy of agent threats
- Real-world validation from the March 2026 ROME incident, where a safety-trained agent autonomously mined cryptocurrency, opened SSH tunnels, and probed internal networks during RL training
- A structural playbook for financial services CISOs: stop assessing intent, monitor action-level telemetry, enforce least-privilege tool binding and ephemeral credentials, and fold AI agents into the insider-threat programs FSIs already run

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

LastPass	Risk Ledger	Silverfort
The identity gap: Closing what AI opened in financial services	**The sectoral resilience mandate: Mapping systemic concentration in the uk Financial Ecosystem**	**Securing the invisible – AD NHI discovery and protection**
Mario Platt, Vice President, CISO, LastPass	**Justin Kuruvilla,** Chief Cybersecurity Strategist, Risk Ledger	**Kev Smith,** EMEA Principal Engineer, Silverfort

Agenda	
11:00	Networking break
11:30	**Securing cloud platforms at scale** **Laura Good,** Cloud Security Architect, Lloyds Banking Group • Challenging legacy security ways of working that don't scale with rapid cloud adoption • Creating security approaches that scale across hundreds of internal teams • What it actually takes to move security from a blocker to an enabler in practice
11:50	**The evidence game: Proving cyber-resilience without slowing the business** **Alan Simpson,** UK and Ireland Field CISO, Rapid7 • Financial services organisations have invested heavily in cyber-visibility, yet many still rely on screenshots, spreadsheets and manual evidence gathering when scrutiny arrives • This session explores how existing security, identity, vulnerability, and service management data can be turned into trusted evidence for audits, regulators, boards and risk committees • Using practical examples, it will show how cyber-teams can prove resilience, reduce disruption for IT, and respond with confidence when pressure increases
12:10	**This was never a drill: The case for autonomous IT** **Dan Jones,** Senior Security Advisor, Tanium • Cyber-threats have crossed a critical threshold. Attackers now identify weaknesses, move laterally, and exploit vulnerabilities faster than traditional security operations were built to handle • The problem is structural. Most security teams still rely on reactive, manual, ticket-driven workflows – while managing sprawling estates across cloud, endpoint, identity, and hybrid infrastructure. The result: a widening gap between threat speed and response capability • This raises a fundamental question: can human-led operations alone defend modern digital environments, or is a more autonomous model now required? • This session explores what a shift toward autonomous IT looks like in practice – from real-time decision-making to self-healing infrastructure – and how organisations can introduce autonomy without sacrificing accountability or control • This session asks: how are AI-driven attacks changing the speed and scale of required response? What does a maturity path toward autonomous, self-healing operations look like? Which decisions should remain human-led – and which can be delegated to machines? If autonomous systems make the wrong call, how quickly can you recover?
12:30	**Zero Trust controls at the endpoint** **Oscar Javier Hernandez Rodriguez,** 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
12:35	**Education Seminars | Session 2** **CyroCyber** **The first time you test crisis decision making shouldn't be during a crisis** **Peter Lane,** Consultancy Director, CyroCyber **Metomic** **The insider you never hired: AI agents and inherited access** **Ben van Enckenvort,** Co-founder & CTO, Metomic **WorkNest** **Third-party compromise – attacks through the suppliers, code and pipelines you already trust** **Dom Mortimer,** Head of Red Team, WorkNest
13:15	Lunch and networking
14:20	**Quantum is coming. Financial services can't afford to wait** **Will Collinson,** 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

Agenda

14:40 — **Trust, then autonomy: Evaluating Agentic AI in financial services institutions**

Chris Vaughan, Solution Engineer, Sublime Security

- The financial sector faces unique risks from AI security tools that can't be explained or audited, with regulations like DORA, FCA resilience requirements, and SR 11-7 making ungovernable AI a compliance liability, not just an operational one
- Correctly measuring and categorising AI autonomy is critical; a practical framework built around transparency, explainability, and auditability is needed to evaluate agentic AI against both security and regulatory standards
- Security and risk teams should leave equipped with the right questions to cut through vendor hype, understand model risk management in practice, and distinguish genuine autonomous AI capability from buzzword-driven marketing

15:00 — **The new non-human insider: Governing the agents**

Kevin Carr, Senior Manager, Solutions Engineering, Drata

- Financial institutions are expected to demonstrate security and operational resilience every day, but most still rely on point-in-time audits, static questionnaires, and fragmented tools
- AI has widened that gap: regulators now expect more current assurance, while the business fills up with agents, APIs, and vendors no one has classified as identities – each a non-human insider with valid credentials and unexamined scope
- This session treats those agents as privileged actors that supervisors will increasingly hold to the same standard as humans
- It examines why annual, manual approaches break under DORA, the PRA and FCA's operational resilience expectations, the EU AI Act, and the UK's incoming Cyber Security and Resilience Bill – and what it takes instead to discover every agent, enforce policy on what it is allowed to do, detect drift in behaviour or permissions, and produce evidence that can stand up on any given day
- We'll also be candid about current limits: data quality, incomplete inventories, humans still on the critical path for approvals and exceptions, and the open questions around governing the agents themselves
- The session closes with a grounded view of the next 18 months – what's realistic, what's still experimental, and where financial institutions should invest now

15:20 — **Education Seminars | Session 3**

ConcentricAI

AI is breaking data security... and fixing it: The new reality of AI-driven risk and how to stay ahead

Stephen Green, Regional Vice President of EMEA, ConcentricAI

Doppel

Disrupting social engineering in financial services: Protect your customers, people, brand, and revenue

Daniel Oxley, Senior Engineer, Doppel

16:00 — Networking break

16:20 — **PANEL DISCUSSION** — **Customer data & AI: Control, exposure, and proof**

Simon Brady, Event Chairman; **Sam Hubery,** BISO, Fidelity International; **Jai Ferguson,** AI Regional Lead – Europe, HSBC; **Dr Narayan Shiva,** CTO and Enterprise Architect, iBANK

- As organisations adopt AI, where are you seeing customer data most commonly interact with this tool and how are you improving visibility over time?
- What controls or approaches are proving most effective in practice for preventing customer data being exposed to AI tools – and where are you still seeing challenges?
- Are you allowing any use of third-party or public AI tools (like ChatGPT) with customer data and what specific safeguards make that acceptable?
- Can you demonstrate that customer data is properly controlled within AI systems?

16:50 — **Rise of autonomous attacks (live Mythos-style hack)**

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

- See how autonomous AI agents are now running the recon and exploitation phases of real-world attacks. and what that means for boards, CISOs, and red teams in 2026
- A first-hand look at how agentic offensive AI works in practice, driven by intent, not step-by-step instruction
- See AI agent run reconnaissance against a controlled target, identify exploitable assets, and demonstrate the early stages of a kill chain in real time
- A walk through real-world findings from recent engagements including critical vulnerabilities discovered by AI agents that automated scanners (Tenable, Qualys, Nessus) had missed for over 18 years
- What defenders need to know: why traditional, control-based security models are structurally insufficient against goal-driven autonomous attackers, and the three specific actions every CISO should be taking before this becomes the default attacker model

17:10 — Chairman's closing remarks

17:15 — Drinks reception & networking

18:30 — End of conference

Education Seminars

ConcentricAI

AI is breaking data security… and fixing it: The new reality of AI-driven risk and how to stay ahead

Stephen Green, Regional Vice President of EMEA, ConcentricAI

AI is rapidly becoming one of the biggest drivers of productivity and innovation in the enterprise – and one of the fastest-growing sources of data security risk. As copilots, assistants, and public AI tools become integrated into daily work, sensitive data is flowing into systems that most security teams can't fully see, understand, or control.

The problem is that traditional data security controls were never built for this. In fact, many organisations were already struggling to operationalise data security before AI accelerated the challenge. The good news? AI isn't just creating the problem – it's also enabling a smarter, more effective way to solve it.

Attendees will learn:

- Why AI has become one of the fastest-growing and least visible sources of enterprise risk
- How GenAI is creating new exposure points for sensitive data
- Why legacy data security tools have failed to keep up – and why AI is making those gaps harder to ignore
- How context-aware, AI-driven data security can deliver more accurate visibility, stronger controls, and real-time enforcement
- What organisations can do to enable AI innovation without expanding their risk surface
- Attendees will leave with a clearer understanding of how AI is reshaping data security – and how they can use that same technology to gain control, minimise exposure, and support safer AI adoption across the business

CyroCyber

The first time you test crisis decision making shouldn't be during a crisis

Peter Lane, Consultancy Director, CyroCyber

Most organisations have an incident response plan. Far fewer know how their leadership teams will actually perform when critical decisions need to be made under pressure. As financial services firms face increasing regulatory scrutiny and more disruptive cyber-incidents, resilience can no longer be proven through documentation alone. The real test is how quickly and effectively an organisation can coordinate, communicate and make decisions when systems, operations and reputation are on the line.

This session explores how cyber-exercising, from executive crisis simulations and Gold/Silver/Bronze command structures through to live play attack scenarios, helps organisations expose gaps before attackers or regulators do.

Attendees will learn:

- We'll examine how leading financial services organisations are using exercising to expose hidden gaps in crisis decision making and escalation paths
- Test how effectively executive, operational and technical teams coordinate under pressure
- Improve speed and clarity of communication during high stakes incidents
- Strengthen confidence in real-world operational resilience
- Align exercising programmes with expectations under the UK Cyber Security & Resilience Bill and CAF 4.0
- A practical discussion for CISOs and senior cyber-leaders looking to build confidence in how their organisation will respond in the face of a cyber-attack

Doppel

Disrupting social engineering in financial services: Protect your customers, people, brand, and revenue

Daniel Oxley, Senior Engineer, Doppel

Financial institutions are facing a new era of fraud driven by AI-powered social engineering attacks that exploit trust across both external channels and human workflows.From impersonated executives and phishing campaigns to deepfake voice calls targeting helpdesks and contact centres, attackers are operating faster across more channels and with greater sophistication than ever before. During this session, Dan will break down how these attacks actually operate and what it takes to stop them.

Attendees will learn:

- How to move beyond fragmented tools and traditional training programs to a unified approach that exposes and eliminates real-world threats
- Through real examples and a live walkthrough of Doppel's platform, you will see how financial institutions can protect customers, strengthen workforce readiness, and reduce fraud and regulatory risk

Education Seminars	
LastPass **The identity gap: Closing what AI opened in financial services** **Mario Platt,** Vice President, CISO, LastPass	This thought-provoking session will challenge assumptions around existing security strategies, revealing how the rapid rise of AI tools, agents, and non-human identities is outpacing traditional controls like MFA and IAM. Through compelling data, real-world case studies, and practical guidance, attendees will gain fresh insight into managing credential sprawl, securing AI-driven environments, and meeting evolving regulatory expectations, equipping them to move beyond the illusion of security and build truly resilient, identity-first protection. **Attendees will learn:** • How to manage credential sprawl • Secure AI-driven environments • Meet evolving regulatory expectations • How to move beyond the illusions of security and build truly resilient, identity-first protection
Metomic **The insider you never hired: AI agents and inherited access** **Ben van Enckenvort,** Co-founder & CTO, Metomic	Most companies have years of overexposed data sitting across countless tools – for many, this has been a sleeping dragon. Today, employees connect Claude, Copilot and other AI tools to their SaaS estate, and a new actor appears: an agent operating with the full permissions of whoever connected it, across every tool it can reach, with no visibility or guardrails over what it can access and what it can do. This session shows where that gap opens, why identity and DLP controls were never built to see it, and how to close it – bringing it to life with a sneak preview of Metomic's AI gateway. **Attendees will learn:** • Where AI agents inherit human access, and how they slip past IAM, DLP and CASB controls • How an AI gateway provides a single point to see and govern what agents do across SaaS, deciding in real time whether to allow, block or escalate a request • What a live view of agent activity reveals about which data is actually being touched, and how little of it most teams can currently see • A layered path to visibility and control with no rip-and-replace, plus language to articulate the risk to the board and where DORA and the UK Cyber Security and Resilience Bill apply
Risk Ledger **The sectoral resilience mandate: mapping systemic concentration in the UK financial ecosystem** **Justin Kuruvilla,** Chief Cybersecurity Strategist, Risk Ledger	While individual financial institutions have historically focused on their own operational perimeters, the true threat to stability lies in the hidden supply chain dependencies that bind the sector together. The UK's evolving Operational Resilience (OPRes) framework, specifically the focus on Critical Third Parties (CTPs), signals a paradigm shift: it is moving beyond firm-specific risk to tackling systemic vulnerabilities. Most organisations remain blind to these shared dependencies at the 3rd-party level and beyond, creating invisible single points of failure that no single firm can identify in isolation. This session explores the regulatory drive to aggregate multi-tier supplier data to map the wider financial ecosystem, and how organisations can collaborate with their peers to proactively identify these shared threats today. **Attendees will learn:** • The regulatory drive to aggregate multi-tier supplier data to map the wider financial ecosystem • How organisations can collaborate with their peers to proactively identify these shared threats today

Education Seminars	
Silverfort **Securing the invisible – AD NHI discovery and protection** **Kev Smith,** EMEA Principal Engineer, Silverfort	Service accounts are one of the most overlooked areas in identity security. They operate continuously in the background, connecting applications and running automated processes across your environment – often with elevated privileges and no human owner actively managing them. This is even more prevalent with frontier models like Mythos leveraging such identities. That's exactly the problem Silverfort was built to solve. Full discovery, behavioural baselining, and real-time enforcement – across your entire environment. **Attendees will learn:** • Discovery and runtime access protection for service accounts is a critical capability for any IAM team operating at scale • Know what you have – discover and prioritise your highest risk service accounts before they become a problem • Get to control fast – no agents, no schema changes, no lengthy deployment; protection that fits around your environment, not the other way round
WorkNest **Third-party compromise – attacks through the suppliers, code and pipelines you already trust** **Dom Mortimer,** Head of Red Team, WorkNest	Organisations increasingly face threat actors who bypass perimeter defences entirely by targeting the third-party suppliers, software libraries, and CI/CD pipelines that already hold trusted access to their environments. This presentation explores how attackers exploit these relationships to achieve high-impact compromises, examining why financial entities are prime targets, the methods adversaries use, and the defensive considerations organisations should be aware of, including how red team engagements can be leveraged as a practical tool for identifying and stress-testing supply chain exposure before a real attacker does. **Attendees will learn:** • How attackers exploit these relationships to achieve high-impact compromises • Why financial entities are prime targets and the methods adversaries use • The defensive considerations organisations should be aware of, including how red team engagements can be leveraged as a practical tool