Post event report

e-Crime & Cybersecurity Germany

18th June 2026, Munich

Strategic Sponsors

1Password

Delinea

rubrik

THREATLOCKER® ZERO TRUST PLATFORM

Education Seminar Sponsors

fileorbis

intruder

RED SIFT

VARONIS

Networking Sponsor

CybelAngel

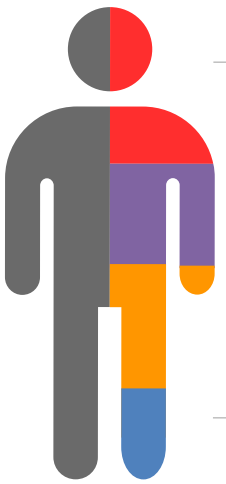
Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

Key themes

- Achieving visibility across ecosystems
- Data integrity a critical priority
- Defending against the latest ransomware variants
- Securing Agentic Al
- Why zero trust, isolation and segmentation are key
- From Analysts to Al Supervisors
- Making the best use of threat intelligence
- Security Posture Management
- Improving continuous attack surface discovery
- The power of automation
- Adversary simulation and behavioural analysis
- 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

Dan Andrew,
Head of Security
Intruder

Jonathan Armstrong,
Partner
Punter Southall Law

Gökhan Aydın,
VP Sales and Business Development
FileOrbis

Nilesh Borole,
IT Security Manager
Golding Capital Partners

Sven Carlsen,
Sales Engineer
Varonis

Gulnara Hein,
CISO
Chintai

Sreedevi Jay,
Global Cyber Security Compliance Manager
Amer Sports

Yair Kler,
Vice President, Security Architecture
DHL Group

Klaus-E. Klingner,
Information Security Officer
Asambeauty

Alejandro Martín Soto,
Head of Digital Security Architecture
Airbus Defence and Space

Billy McDiarmid,
VP, Customer Engineering
Red Sift

John McNamee,
Sales Team Lead
ThreatLocker

Andreas Scheurle,
Enterprise Account Executive
Delinea

Geoffrey Taylor,
Information Security Officer
Nordea Asset Management

Agnès Terreau,
Country DPO & Security Officer
ManPower Group

Stefan Wiechers,
Enterprise Sales Engineer
Rubrik

Natalie Williams,
Enterprise Sales Leader, EMEA
1Password

Adeiza Yisa,
Business Information Security Office
Shell

Agenda

08:30 Registration & breakfast networking

09:30 Chairman's welcome

09:40 **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

10:00 **Knowledge is the best defence: What do you know about identities?**

Andreas Scheurle, Enterprise Account Executive, Delinea

- Identify all identities and their risk for you within your organisation
- AI is on everyone's lips: What does AI do with your identities?
- Manage permissions for your critical accounts
- How to easily bring knowledge into real policies and actions

10:20 **The challenge of securing AI on a global scale**

Yair Kler, Vice President, Security Architecture, DHL Group

- Learn how CISOs can enable responsible AI adoption by advancing innovation without resorting to a blanket 'no' while preserving strong security foundations
- Understand how FOMO-driven AI adoption is pressuring enterprises into rapid, high-risk decisions while bypassing established best practices
- Addressing the issue of emerging AI-specific threat classes such as prompt injection and why they create new risks that remain difficult to mitigate
- Recognising how long-standing security challenges like secrets management and identity lifecycle governance are re-emerging with greater complexity in AI-driven environments

10:40 **Education Seminars | Session 1**

Red Sift **Security maturity before the wake-up call: How to protect your domain estate** **Billy McDiarmid,** VP, Customer Engineering, Red Sift	**Varonis** **Robot vs. Robot – Defending against AI-driven cyber-attacks** **Sven Carlsen,** Sales Engineer, Varonis

11:20 Networking break

11:50 **PANEL DISCUSSION** **Beyond compliance — Building cyber-resilience that actually works**

Jonathan Armstrong, Partner, Punter Southall Law (Moderator); **Gulnara Hein,** CISO, Chintai;
Sreedevi Jay, Global Cyber Security Compliance Manager, Amer Sports;
Nilesh Borole, IT Security Manager, Golding Capital Partners; **Klaus-E. Klingner,** Information Security Officer, Asambeauty

- 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?

12:20 **Resilience for everything: How to ensure business continuity across cloud, identity, and AI**

Stefan Wiechers, Enterprise Sales Engineer, 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

Agenda

12:40 — **Your identity security architecture was built for humans. It's time for a reset**

Natalie Williams, Enterprise Sales Leader, EMEA, 1Password

- A year ago, managing access for AI agents was a theoretical question. Today, NHIs aren't at the gate; they're inside the perimeter, acting autonomously and often invisibly
- Now, leaders must embrace a new paradigm of identity security – one that responsibly governs access for non-human identities
- This session will discuss 1Password's identity security framework, and how to apply bedrock security principles to a radically altered landscape

13:00 — Lunch and networking

14:00 — **AI and IT/OT convergence – When models meet motors: AI at the IT/OT edge**

Adeiza Yisa, Business Information Security Office, Shell

- Understand what IT/OT convergence really means in practice and what value AI brings to the mix
- Learn the key architectural and security considerations for integrating AI with legacy IT/OT convergence
- Hear about real-world use cases and measurable outcomes

14:20 — **Zero Trust controls at the endpoint**

John McNamee, Sales Team Lead, 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

14:25 — **Education Seminars | Session 2**

FileOrbis	Intruder
Visibility, governance, and control: Protecting enterprise content across files, M365, and AI	**Your perimeter is on the front lines: Attack surface reduction as a primary defence**
Gökhan Aydın, VP Sales and Business Development, FileOrbis	**Dan Andrew,** Head of Security, Intruder

15:05 — Networking break

15:35 — **Effective data breach management**

Agnès Terreau, Country DPO & Security Officer, ManPower Group

- How to respond effectively during the first critical hours of a data breach
- Common pitfalls that cause incidents to escalate and how to avoid them
- The importance of clear roles, escalation, and communication during incidents
- How organisational culture and decision-making influence breach outcomes and overall impact

15:55 — **PANEL DISCUSSION** **The corporate security case for AI sovereignty**

Jonathan Armstrong, Partner, Punter Southall Law (Moderator);
Alejandro Martín Soto, Head of Digital Security Architecture, Airbus Defence and Space;
Yair Kler, Vice President, Security Architecture, DHL Group; **Adeiza Yisa,** Business Information Security Office, Shell

- 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?

16:25 — Chairman's closing remarks

16:30 — End of conference

Education Seminars

FileOrbis

Visibility, governance, and control: Protecting enterprise content across files, M365, and AI

Gökhan Aydın, VP Sales and Business Development, FileOrbis

As enterprise content becomes increasingly distributed across file servers, Microsoft 365, cloud platforms, and different storages, organisations face growing challenges around visibility, governance, and control. Sensitive information is often scattered across multiple repositories, shared beyond intended audiences, or fed into AI systems without sufficient oversight.

Attendees will learn:

- Why securing enterprise content requires more than traditional file storage or access management
- How organisations can gain visibility into where content resides, understand what types of sensitive data they have, and apply consistent governance policies across files, Microsoft 365, and AI environments
- The importance of content-aware controls, secure sharing, automated remediation, compliance, and centralised management in reducing risk while supporting productivity
- From unstructured data on file servers to collaboration in Microsoft 365 and emerging AI use cases, this discussion will provide practical insights into how enterprises can better protect, govern, and control their content everywhere

Intruder

Your perimeter is on the front lines: Attack surface reduction as a primary defence

Dan Andrew, Head of Security, Intruder

This education seminar will provide a deep-dive into core concepts and practical recommendations for Attack Surface Management (ASM) and asset discovery. Your perimeter is on the front line, and good patch management alone is not enough to protect it. You should leave this session with a better idea of how to blend ASM and asset discovery with patch management for a robust exposure management process.

We'll run through examples of attack surface risks, real-world vulnerabilities affecting internet exposed tech, and why implementing an ASM process is critical alongside patch management. It may be tempting to fall back on just patching your biggest 'known' threats, but some of the biggest risks are vulnerabilities that are not yet publicly known. These threats do not have a CVSS score, and attack surface management is your primary defence. Learn how to future-proof your perimeter.

Asset discovery is also an essential part of managing your attack surface. Keeping track of your internet exposed IPs and domains is far from trivial, and cloud environments in particular make this challenge harder. Losing track of some of your assets is no longer an embarrassing mistake – it's an unavoidable reality. We will show some examples of how this happens, and give a practical approach to asset discovery which helps you keep track, and avoid systems slipping outside of your exposure management process entirely.

Attendees will learn:

- Integrating Attack Surface Management into your patch management process – defining ASM as a primary defence that's proactive, not reactive
- Prioritisation considerations and why informational risks are criticals waiting to happen. Why not all 'criticals' are equal, and why CVSS is not king
- The importance of asset discovery to find shadow IT and build a realistic view of your attack surface. Practical recommendations on how to approach this

Education Seminars	
Red Sift **Security maturity before the wake-up call: How to protect your domain estate** **Billy McDiarmid,** VP, Customer Engineering, Red Sift	Most organisations don't mature their email and domain security because they always follow government frameworks or industry standards. It comes after their nurture sequences started landing in spam after Google and Yahoo's 2024 enforcement changes, a journalist found a forgotten subdomain redirecting to a gambling site, or a customer called to report receiving a replicated invoice from a lookalike domain. What the board calls 'maturity' is usually just scar tissue with a budget attached. The uncomfortable truth? Most organisations don't know how many domains they actually own, who's sending email on their behalf, and what subdomains still exist out there. **Attendees will learn:** • What a domain estate looks like from the outside, using live research to show where the gaps really are and how to get ahead of the next incident • This session introduces a practical maturity framework, from basic asset visibility to full certificate and DNS hygiene for full-spectrum defence
Varonis **Robot vs. Robot – Defending Against AI-driven cyber-attacks** **Sven Carlsen,** Sales Engineer, Varonis	AI-based cyber-attacks are evolving faster than any human threat ever could. Phishing, identity abuse, and data exfiltration now happen in seconds – fully automated and massively scaled by autonomous algorithms. In this new 'Robot vs. Robot' era, traditional security approaches are no longer sufficient. Organisations need a fundamentally different defence strategy – one that understands and protects what attackers are truly after: data. A data security platform is required to detect attacker behaviour early – often before damage occurs. By combining machine learning–based threat detection, automated least-privilege enforcement, and full visibility across critical data, identities, and access paths, DSPM enables organisations to stay ahead of AI-powered threats. **Attendees will learn:** • Why AI-driven attacks render traditional security controls ineffective and create unprecedented risk around sensitive data • How organisations can gain full visibility into data, permissions, and user behaviour across M365, file systems, and cloud environments • How machine learning and behavioural analytics help detect threats early – before data is exfiltrated • The role of automated least-privilege and continuous remediation in reducing attack surfaces at scale • When attacks are driven by machines, defence must be faster, smarter, and laser-focused on what matters most: data