Post event report

Principal Sponsor

Opensystems | P

Strategic Sponsors

CLOUDFLARE

Delinea

rubrik

THREATLOCKER® ZERO TRUST PLATFORM

Education Seminar Sponsors

fileorbis

Branding Sponsors

eye.

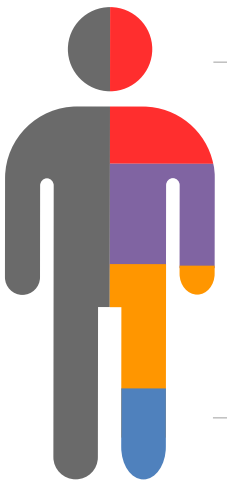
Honeywell

Inside this report:

Key themes

- 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
- Achieving visibility across ecosystems
- Transitioning OT to the Cloud?
- Defending against the latest ransomware variants
- OT and the regulations
- Why zero trust, isolation and segmentation are key
- Pen testing for OT/SCADA

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 Engineering Manager
Rubrik

Nikolaus Brandstetter,
Group CISO
MM Group

Julian Dube,
Information Security Officer
E.ON Digital Technology

Ivo Friedberg,
Head of Cyber Defense &
Shared Services
Austrian Power Grid AG

John McNamee,
Sales Team Lead
ThreatLocker

Andreas Mueller,
Regional Sales Director CEUR
Delinea

Utz Nisslmüller,
Security Specialist
City of Vienna

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

Daniele Sangion,
CISO & CSO
UniCredit Bank Austria

Sebastian Scherl,
SASE GTM Lead DACH
Cloudflare

Cornelius Schneider,
Governance, Risk and
Compliance Manager
E.ON Digital Technology

Gerald Schremser,
Group CISO
Prinzhorn Group

Stefan Schweizer,
Senior Vice President Sales Europe
Open Systems

Geoffrey Taylor,
Information Security Officer
Nordea Asset Management

Mert Topaloglu,
Presales Manager
FileOrbis

José Torre,
CISO & Data Privacy &
Compliance Manager
A1 Digital

Agenda	
08:30	Breakfast networking break
09:30	Chair's opening remarks
09:40	**Secure your supply chain – An NIS2 imperative for resilience** **Geoffrey Taylor,** Information Security Officer, Nordea Asset Management • Understanding how rising supply chain attacks threaten organisations and why this is a core focus under NIS2 • Recognising how evolving regulatory requirements are driving renewed emphasis on third-party risk management • Adopting a proactive, risk-based approach beyond compliance to strengthen supply chain resilience
10:00	**Balancing innovation, stability, and security in modern IT landscapes** **Stefan Schweizer,** Senior Vice President Sales Europe, OpenSystems • Navigating the trade-offs between innovation speed, operational resilience, and enterprise rise • Positioning cybersecurity as a driver of business value, trust, and competitive advantage • Strengthening governance and accountability to meet rising regulatory and compliance demands • Enabling scalable, secure growth across hybrid environments through platform-driven strategies
10:20	**Resilience for everything: How to ensure business continuity across cloud, identity, and AI** **Gary Adams,** Sales Engineering Manager, 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
10:40	**One security vision: Uniting E.ON's subsidiaries through standardisation** **Julian Dube,** Information Security Officer, E.ON Digital Technology, and **Cornelius Schneider,** Governance, Risk and Compliance Manager, E.ON Digital Technology • How to standardise security across diverse subsidiaries with unique structures and requirements • Applying the Central Governance Framework as the blueprint for IT and OT alignment • Preparing subsidiaries through onboarding and central service integration • Aligning leadership and objectives to achieve group-wide transparency and security consistency
11:00	Networking break
11:30	**FIRESIDE CHAT: Securing systems we can't switch off** Event Chairman; **Ivo Friedberg,** Head of Cyber Defense & Shared Services, Austrian Power Grid AG • Where does traditional cybersecurity best practice break down in industrial OT environments, and how do you design security for systems that cannot simply be stopped, rebooted, or patched in the usual way? • In critical infrastructure environments, where cyber-risk, safety, engineering integrity, and physical consequences are tightly interconnected, how do you ensure clear ownership of risk rather than it sitting ambiguously between cyber, engineering, and operations? • What does it mean in practice to operate systems that other sectors, supply chains, and communities depend on, and how does that responsibility influence your approach to cyber-resilience and OT protection? • Have you made (or had to make) any tough or even controversial decisions around your cybersecurity or security architecture recently?
12:00	**AI safety first: Securing the AI explosion with Cloudflare SASE** **Sebastian Scherl,** SASE GTM Lead DACH, Cloudflare • Why AI is redefining modern network architecture • Secure AI access – without compromising data or control • Take control of MCP servers: Stop Shadow AI before it starts

Agenda

12:20 — **Knowledge is the best defence: What do you know about identities?**

Andreas Mueller, Regional Sales Director CEUR, 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 easy bring knowledge into real policies and actions

12:40 — Lunch networking break

13:40 — **Third-party & outsourcing risk management – Focus on cybersecurity and operational resilience**

Daniele Sangion, CISO & CSO, UniCredit Bank Austria

- Risks you don't see until it's too late
- Cyber-exposure beyond your perimeter
- Resilience that must work under stress, not just on paper
- Decisions that boards expect – and regulators will test

14:00 — **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

14:05 — **Ransomware 3.0: Weaponising AI for the next generation of ransomware attacks**

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

- LIVE DEMO – Inside the first AI-powered ransomware attack – See how my custom Agentic Ransomware Gang can take down a network in under 8 mins
- First-hand insights from real-world red team ops – from legacy tech and broken access controls to the critical lack of real-world security testing
- Why traditional security fails – compliance checklists and conventional tools don't stop modern ransomware
- What CISOs and security leaders must do now – real-world, field-tested steps to prove your controls work before attackers do it for you

14:25 — **Education Seminars | Session 1**

FileOrbis	**Open Systems**
Visibility, governance, and control: Protecting enterprise content across files, M365, and AI	**Balancing innovation, stability, and security in practice**
Mert Topaloglu, Presales Manager, FileOrbis	**Stefan Schweizer,** Senior Vice President Sales Europe, Open Systems

15:05 — Networking break

15:30 — **PANEL DISCUSSION** — **Third party (and beyond) — Where modern breaches begin**

Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England (Moderator);
Nikolaus Brandstetter, Group CISO, MM Group;
José Torre, CISO & Data Privacy & Compliance Manager, A1 Digital;
Utz Nisslmüller, Security Specialist, City of Vienna;
Gerald Schremser, Group CISO, Prinzhorn Group

- How do you identify and manage single points of failure within subcontracting and fourth-party relationships?
- When in-house AI is tightly governed, how do you manage the risks introduced by AI embedded in third-party tools and add-ons?
- What strategies are most effective for detecting and preventing shadow IT and shadow procurement?
- How do you drive cultural change to strengthen and streamline the third-party onboarding process?

16:00 — Chair's closing remarks — **16:10** — End of conference

Education Seminars	
FileOrbis **Visibility, governance, and control: Protecting enterprise content across files, M365, and AI** **Mert Topaloglu,** Presales Manager, 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
Open Systems **Balancing innovation, stability, and security in practice** **Stefan Schweizer,** Senior Vice President Sales Europe, Open Systems	In an increasingly complex and regulated IT landscape, organisations face the challenge of balancing innovation speed, operational stability, and security. Rising cyber-threats, hybrid infrastructures, and growing compliance pressure demand new approaches – where cybersecurity is no longer just a protective function, but an integral part of business strategy. **Attendees will learn:** • How to strategically balance innovation, stability, and security • Why cybersecurity must be treated as a business enabler – not just a protective measure • The role of governance, transparency, and automation in building an effective security strategy • How modern platform approaches unify security, compliance, and performance across hybrid environments