Post event report

e-Crime & Cybersecurity Nordics

23rd April 2026, Stockholm

Strategic Sponsors

censys

Delinea

HORIZON3.ai

rubrik

SOCRadar® Your Eyes Beyond

THREATLOCKER® ZERO TRUST PLATFORM

Education Seminar Sponsors

fileorbis

netskope

Networking Sponsors

1Password

CyberProof® A UST Company

Panorays

Executive Roundtable Sponsors

CyberProof® A UST Company

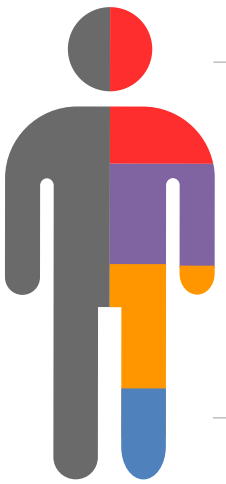
SOCRadar® Your Eyes Beyond

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

Chris Dearden, Lead Sales Engineer
Delinea

William Dixon,
Associate Fellow, Royal United Services Institute and Senior Technology Cyber Fellow
The Ukraine Foundation

Dzana Dzemidzic, BISO
Swedbank AB

Jonas Gyllenhammar,
Sr. Sales Engineer
Censys

Christof Jacques, Solutions Architect
Horizon3.ai

Björn Johrén,
Head of Security & IT Operations
Max Matthiessen AB

Sami Laurila,
GTM Leader Northern Europe Identity & AI Technology
Rubrik

Marcus Lenngren,
Area Manager & Cyber Security Manager
H&M Group

Heléna Malm, Head of CSO Office
Swedbank AB

Andy Quaeyhaegens,
Consultant Channel Solutions Engineer
Netskope

Hanna Rasch,
Information Security & Product Cybersecurity Manager, Production & Logistics
Scania

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

Samet Sazak,
Senior Solutions Engineer
SOCRadar

Martin Solang, Sales Director Nordics
Censys

Geoffrey Taylor,
Information Security Officer
Nordea Asset management

Mert Topaloglu, Presales Manager
FileOrbis

Sean Whelan,
Enterprise Account Executive
Threatlocker

Timo Wiander,
Information Security Manager
LocalTapiola

Agenda	
08:30	Registration and breakfast networking
09:30	Chair's welcome
09:40	**Secure your supply chain – Secure your organisation**
	Geoffrey Taylor, Information Security Officer, Nordea Asset management • Understanding how rising supply chain attacks threaten organisations and how to prevent supplier compromise • Recognising regulatory requirements driving renewed emphasis on effective supply chain management • Adopting a proactive, risk-based approach beyond basic compliance to strengthen supply chain resilience
10:00	**From reactive alert management to proactive internet intelligence**
	Martin Solang, Sales Director Nordics and **Jonas Gyllenhammar,** Sr. Sales Engineer, Censys • Beyond static indicators: Why relying solely on traditional IoCs (Indicators of Compromise) is no longer enough to outpace modern threats • High-fidelity infrastructure visibility: Using enriched threat data to gain deeper insights into attacker environments and emerging risks • Context-driven detection: Leveraging superior data quality to identify patterns and reduce exposure before an incident occurs • Shift to anticipation: Moving away from reactive alert fatigue toward a strategy of disrupting threats before they impact the organisation
10:20	**Identity is the new perimeter: Combine prevention and recovery to ensure organisational survivability during and after an attack**
	Sami Laurila, GTM Leader Northern Europe Identity & AI Technology, Rubrik • Data & identity focus: How to implement robust cyber-recovery and threat containment across your data and identity estate • Beyond prevention: Ensure rapid response and recovery to minimise downtime and business disruption • Stay operational under attack: How zero-trust architecture helps you maintain control and protect critical data – even during ransomware events
10:40	**From awareness to accountability: Building a security culture that lasts**
	Heléna Malm, Head of CSO Office, Swedbank AB and **Dzana Dzemidzic,** BISO, Swedbank AB • Learn how human behaviour drives most security incidents and how strengthening engagement, empowerment, and culture supports secure behaviours beyond technology • Learn how Swedbank integrates people and culture into its security strategy through real challenges, tested solutions, and key organisational insights • Learn how to embed security into everyday business operations, strengthen long-term behavioural change, and build shared ownership for a sustainable security culture
11:00	Networking break
11:30	**Kill the click: DNS blocking that shut down scams at scale**
	Timo Wiander, Information Security Manager, LocalTapiola • How cross-industry collaboration reduced customer fraud losses by up to 70% • Why stopping fraud before the customer clicks changes the economics of fraud prevention • Navigating regulatory barriers • Scaling across operators and markets to protect customers
11:50	**Securing every identity: Humans, machines, and AI**
	Chris Dearden, Lead Sales Engineer, Delinea • In today's cloud-first, remote-work era, traditional network perimeters have dissolved – identity has become the primary attack surface, with over 80% of breaches involving compromised credentials • This session explores how modern enterprises can secure all identity types – from IT admins to developers to AI agents – using Delinea's unified, AI-powered platform • Learn how intelligent, centralised authorisation reduces risk, ensures compliance, and enables secure innovation across your hybrid environment

Agenda

12:10 — Zero Trust controls at the endpoint

Sean Whelan, Enterprise 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

12:15 — Education Seminars | Session 1

FileOrbis
Visibility, governance, and control: Protecting enterprise content across files, M365, and AI
Mert Topaloglu, Presales Manager, FileOrbis

Netskope
Sweden under attack: A blueprint for ProAIctive defence
Andy Quaeyhaegens, Consultant Channel Solutions Engineer, Netskope

12:55 — Lunch networking break

14:00 — Cyber-leadership in an era of dis-cooperation

William Dixon, Associate Fellow, Royal United Services Institute and Senior Technology Cyber Fellow, The Ukraine Foundation

- How global trade fragmentation impacts the community
- How the 'America First' foreign policy is leading to cyber-instability
- Actions the Cyber C-Suite can take

14:20 — AI impact in threat intelligence: What's changed in our life?

Samet Sazak, Senior Solutions Engineer, SOCRadar

- How AI and large language models have changed day-to-day threat intelligence work
- Practical examples of how defenders use AI to analyse underground forums, detect brand abuse, and prioritise real risk faster
- How threat actors abuse AI, including tools like WormGPT, AI-generated phishing, and automated reconnaissance
- What still requires human judgment in threat intelligence, and how to avoid over-trusting AI-driven insights

14:40 — In the cyber-trenches: War stories from 200,000 pentests

Christof Jacques, Solutions Architect, Horizon3.ai

- To defeat the adversary, we must move beyond tracking their tools – we must understand their mind
- The traditional approach to cybersecurity has focused relentlessly on the technical what (malware signatures, TTPs) and the macro why (geopolitical tension, economic drivers)
- However, the next decisive frontier in intelligence and defence requires a pivot to the who: the personality dynamics that fuel cyber-threat actor groups and using autonomous tools to follow in their footsteps
- This plenary will cover what 200,000 real attacks taught us that your security stack probably missed, why attackers keep winning (and how to start thinking like they do), and how autonomous pentesting is changing the economics of defence

15:00 — 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

15:20 — Networking break

15:50 — PANEL DISCUSSION — Beyond compliance — Building cyber-resilience that actually works

Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England (Moderator); **Björn Johrén,** Head of Security & IT Operations, Max Matthiessen AB; **Marcus Lenngren,** Area Manager & Cyber Security Manager, H&M Group; **Hanna Rasch,** Information Security & Product Cybersecurity Manager, Production & Logistics, Scania

- 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?

16:20 — Chair's closing remarks

16:30 — 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
Netskope **Sweden under attack: A blueprint for ProAIctive defence** **Andy Quaeyhaegens,** Consultant Channel Solutions Engineer, Netskope	With Swedish enterprises under constant fire from AI-powered threats, protecting your assets requires more than a firewall. Learn how Netskope's context-aware security moves you from static 'No' to intelligent 'Know,' providing full data control across the AI frontier. Don't just defend; take the AI fast lane with confidence **Attendees will learn:** • Neutralising AI threats: Master strategies to counter high-velocity, automated attacks on Swedish infrastructure • Intelligent data control: Shift from 'No' to 'Know' with context-aware security for GenAI • The ProAIctive Blueprint: Practical steps to safely accelerate AI adoption without compromising security