Post event report

e-Crime & Cybersecurity Nordics

28th January 2026, Helsinki

Strategic Sponsors

censys

Delinea
Securing identities at every interaction

Ping Identity

rubrik

SOCRadar®
Your Eyes Beyond

THREATLOCKER®
ZERO TRUST PLATFORM

Education Seminar Sponsors

Commvault®

Filigran

Networking Sponsor

CyberProof®
A UST Company

Executive Roundtable Sponsors

CyberProof®
A UST Company

SOCRadar®
Your Eyes Beyond

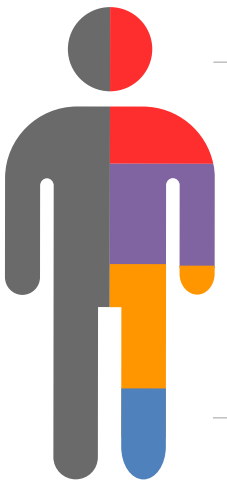
Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

Key themes

- What do regulators really want?
- Pen testing for OT / SCADA
- Transitioning OT to the Cloud?
- Achieving visibility across ecosystems
- Dealing with regulations
- Adversary simulation and behavioural analysis
- The power of automation
- Improving continuous attack surface discovery
- Security posture management
- Defending against the latest ransomware variants
- Making the most of AI and ML
- Developing the next generation of security leaders
- Cybersecurity as a service: the pros and cons
- Cybersecurity for SaaS/IaaS/PaaS
- Why zero trust, isolation and segmentation are key
- Making the best use of threat intelligence
- Building a next gen security architecture
- OT and the 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

Samuli Bergström, Director, Head of CSIRT at Traficom
NCSC-FI

Ashish Bhadouria, Domain Engineering Manager – Security & Privacy
Ingka Group

Simon Brady, Chairman
AKJ Associates

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

Santtu Erkkilä, Cyber Governance, Risk & Compliance Lead
Neste

Jonas Gyllenhammar, Senior Sales Engineer
Censys

Kari Keinänen, CISO
Lounea Oyj

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

Sachin Loothra, Lead Solutions Architect
Telia

Karsten Dreyer Lund, Channel Solutions Engineer
Commvault

Magnus Lundgren, Sales Director Nordics
Filigran

Fidel Nozal, Account Executive
ThreatLocker

Jay Prakash, CISO
Paf

Samet Sazak, Senior Solutions Engineer
SOCRadar

Scott Shields, Enterprise Sales Engineer
Delinea

Jeevan Singh, Head of Cyber Security & Common Infrastructure Services
Nokia Technology Standards

Martin Solang, Sales Director Nordics & Benelux
Censys

Marcin Zimny, Senior Principal Solution Architect
PingIdentity

Agenda	
08:00	Breakfast networking break
09:00	Chair's opening remarks
09:10	**What lies ahead in 2026?**
	Samuli Bergström, Director, Head of CSIRT at Traficom, NCSC-FI • What Finland's cyber-threat landscape looks like right now and we are navigating • What attacks organisations are dealing with right now • Stay ahead: Upcoming threat trends and how to be prepared
09:30	**The future of cyber-resilience: Securing the exposed edge of critical infrastructure**
	Martin Solang, Sales Director Nordics & Benelux, Censys & **Jonas Gyllenhammar,** Senior Sales Engineer, Censys • Growing attack surface: Connectivity expands exposure across services, ports, and unmanaged assets • Internet exposure insights: What Censys data reveals about today's misconfiguration trends • Attacker speed: How adversaries find and exploit exposures within minutes • Proactive resilience: Using continuous ASM to secure the exposed edge early
09:50	**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
10:10	**Why quantum cryptography isn't really a technology problem**
	Rune Espensen, Head of Information Security Office, Nordea • Why quantum computing is a society-wide challenge and how its impact extends far beyond purely technical concerns • Learn why preparation must start now and what early actions reduce long-term risk as quantum capabilities advance • Discover why technology isn't the main barrier and what organisational, cultural, and strategic shifts are required to navigate the quantum transition effectively
10:30	Networking break
11:00	**Zero Trust in action: Policy-driven access for cyber-resilience**
	Sachin Loothra, Lead Solutions Architect, Telia • Rising cyber-threats and their impact on organisational resilience • Policy-driven access as the foundation for Zero Trust implementation • How Zero Trust reduces breach impact and ensures business continuity
11:20	**Unmasking fraud. The lifecycle and operational dynamics of identity deception**
	Marcin Zimny, Senior Principal Solution Architect, PingIdentity • In this session, you will learn how identity deception like synthetic identities, new account fraud, and AI driven account takeovers is reshaping the fraud landscape • We will walk through the full lifecycle of these attacks and show how they exploit operational blind spots in traditional fraud defences. You will see why legacy and siloed tools fall short, and how a modern identity first approach can detect threats in real time, adapt access journeys based on risk, and stop fraud without disrupting legitimate users • If you are looking to reduce losses and rebuild digital trust, this session will give you a practical blueprint to do just that

Agenda

11:40 — **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

11:45 — **Education Seminars**

Commvault	**Filigran**
From defensive security to cyber-resiliency	**Utilise your threat intelligence to improve your security posture, continuously!**
Karsten Dreyer Lund, Channel Solutions Engineer, Commvault	**Magnus Lundgren,** Sales Director Nordics, Filigran

12:25 — Lunch networking break

13:30 — **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

13:50 — **Privileged identities: The front door of modern cyber-attacks**

Scott Shields, Enterprise Sales Engineer, Delinea

- Why privileged identities are the gateway for today's advanced threats
- Beyond vaulting – learn how to eliminate standing privilege and naturally build cyber-resilience
- How does identity security help evolving regulations like NIS2 and DORA
- Why unified, platform-based PAM strategies are key to sustaining both security and speed

14:10 — **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

14:30 — **How Neste built a business-driven cyber-risk program**

Santtu Erkkilä, Cyber Governance, Risk & Compliance Lead, Neste

- Understand the key challenges Neste faced in managing cyber-risk across a global, complex industrial and R&D environment
- See the step-by-step journey of transforming their cyber program into one that is business-driven and risk-informed
- Learn the lessons from Neste's experience that you can apply to mature your own organisation's risk management program

14:50 — Networking break

15:20 — **PANEL DISCUSSION** — **Building resilient cyber-risk management**

Simon Brady, Chairman, AKJ Associates (Moderator); **Jay Prakash,** CISO, Paf; **Ashish Bhadouria,** Domain Engineering Manager – Security & Privacy, Ingka Group; **Jeevan Singh,** Head of Cyber Security & Common Infrastructure Services, Nokia Technology Standards; **Kari Keinänen,** CISO, Lounea Oyj

- How can organisations turn risk appetite statements and metrics into practical decision-making tools?
- With NIS2 and similar regulations, what does 'appropriate and proportionate' really look like in practice – and how can risk management guide the response?
- What makes for strong cyber-risk metrics, and how can CISOs and CSOs give the Board real confidence in the organisation's risk posture?
- How does a resilience-first mindset shift culture – from blame and prevention to acceptance, preparedness, and recovery?

15:55 — Chair's closing remarks

16:00 — End of conference

Education Seminars

Commvault

From defensive security to cyber-resiliency

Karsten Dreyer Lund, Channel Solutions Engineer, Commvault

In today's threat landscape, where ransomware has become a $57 billion global crisis, traditional security models are proving insufficient. Organisations are investing heavily in prevention, yet breaches continue to occur – highlighting a critical gap between security plans and recovery readiness. This session explores the fundamental shift from defensive security to cyber-resilience, examining why prevention alone isn't enough and how organisations can prepare for – and assume – breach. We will discuss practical frameworks for building recovery readiness, the critical differences between disaster recovery and cyber-recovery, and why testing your ability to restore operations is just as important as preventing attacks in the first place.

Attendees will learn:

- Understand the 'assume breach' paradigm – Why traditional security investments focus on prevention while recovery readiness remains critically underdeveloped, and how to rebalance your resilience strategy
- Distinguish cyber recovery from disaster recovery – Learn the fundamental differences in scope, goals, and methods between operational recovery, disaster recovery, and cyber recovery scenarios
- Build and test your minimum viable company – Identify which critical applications and systems you need to resume operations, and why frequent testing is essential to validate recovery readiness
- Shift your success metrics – Move beyond traditional RTO/RPO to Mean Time to Clean Recovery (MTCR) and understand why identifying your last clean backup point is critical to cyber-resilience

Filigran

Utilise your threat intelligence to improve your security posture, continuously!

Magnus Lundgren, Sales Director Nordics, Filigran

In today's dynamic threat landscape, collecting threat intelligence feeds is no longer enough. Organisations must transform raw data into actionable insights by aligning intelligence with critical assets and business risks. This approach ensures that security teams prioritise what truly matters, reducing noise and focusing on threats that pose the greatest impact. Breaking down operational silos is essential, integrating intelligence sharing across SOC, CTI, vulnerability management, and leadership fosters collaboration and accelerates decision-making. When these teams work in harmony, organisations can respond faster and more effectively to emerging threats.

A robust security posture requires more than one-time improvements; it demands continuous refinement. Establishing a feedback loop between threat intelligence, detection engineering, and security validation creates a cycle of measurable progress. This iterative process enables organisations to adapt to evolving adversary tactics while validating the effectiveness of their defences. By embedding intelligence into detection and validation workflows, security teams can proactively identify gaps and strengthen resilience.

To operationalise these practices at scale, organisations need flexible, transparent platforms, not rigid, black-box solutions. Filigran's open, collaborative intelligence platform empowers teams to share, enrich, and act on intelligence seamlessly. Its design promotes interoperability and scalability, ensuring that threat intelligence becomes a living, breathing component of your security strategy rather than a static feed. With Filigran, organisations can orchestrate intelligence-driven workflows that unify stakeholders, enhance visibility, and deliver tangible improvements in risk reduction. Continuous improvement is not a luxury, it's a necessity. By leveraging threat intelligence strategically, breaking down silos, and embracing open collaboration, organisations can stay ahead of adversaries and build a security posture that evolves as fast as the threats they face.

Attendees will learn:

- Don't just collect threat intel feeds – drive context and priority from it and align it with your organisation's critical assets and business risks
- Break down silos – orchestrating intel sharing across SOC, CTI, vulnerability management, and leadership, enabling faster, better-informed decisions
- Establish a continuous feedback loop – between threat intelligence, detection engineering, and security validation to drive measurable improvements in security posture
- Leverage Filigran's open, collaborative intelligence platform to operationalise these practices at scale, without locking yourself into rigid, black-box tooling