

Post event report



e-Crime & Cybersecurity Nordics

20th October 2026, Copenhagen

Strategic Sponsors

Delinea



THREATLOCKER
ZERO TRUST PLATFORM

Education Seminar Sponsors



CATO
NETWORKS



Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars

Key themes

AI and quantum

Identity, authority, and control for non-human actors

Data protection and leakage risks

AI anti-phishing and social engineering defences

Who needs to be quantum-ready?

Integrity and the AI-enabled supply chain

Intelligent Threat Detection

Building better security

Making the best use of threat intelligence

Security posture management

Improving continuous attack surface discovery

The power of automation

Adversary simulation and behavioural analysis

Securing the Cloud: still a problem

Best practice fundamentals

Achieving visibility across ecosystems

Transitioning OT to the Cloud?

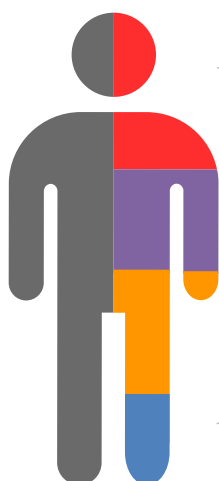
Defending against the latest ransomware variants

Securing the basics

Why zero trust, isolation and segmentation are key

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

Ann-Sophie Barrington,
CISO

JP/Politikens Hus

Nicolai Borchorst,
Senior Sales Engineer

Rubrik

Simon Brady

AKJ Associates

Maria Christiansen,
Head of Applied AI

TDC NET

Chris Dearden,
Lead Sales Engineer

Delinea

Rachel Eldridge,
Solutions Engineer

BeyondTrust

Rune Espensen,
Head of Information Security Office

Nordea

Ben Hanson,
Field CSO

Zenity

Philip Jacobs,
Principal Intelligence Solutions Advisor

Intel 471

Jan Jans,
Legal Counsel

Finanstilsynet (Danish Financial Supervisory Authority)

Robin Johns,
WW AI Security SME

Cato Networks

Martin Kofoed Høding,
VP of Cybersecurity & CISO

SAS – Scandinavian Airlines

Ulf Larsson,
Security CTO

SEB

Lars Liljeroth,
Solutions Engineer

Netskope

Magnus Lundgren,
Sales Director Nordics

Filigran

John McNamee,
Sales Manager

ThreatLocker

Marcus Mølleskov,
Chief Risk & Compliance Officer

Januar

Matt Percival,
Regional VP of Sales

Horizon3.ai

Geoffrey Taylor,
Information Security Officer
Nordea Asset Management

Agenda	
08:00	Breakfast networking and registration
08:50	Conference 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	In the cyber-trenches: War stories from 300,000 pentests – legacy defence misses the modern threat Matt Percival , Regional VP of Sales, 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. - Assume less; validate more. Security teams can miss obvious weaknesses when they focus on the wrong signals. The answer is to prove security through realistic attack paths not simply declare an environment secure. - Think like the attacker. Effective defence requires understanding both how attackers operate and what motivates them from status-seeking and manipulation to thrill-seeking behaviour. - Turn attacker perspective into continuous action. Autonomous pentesting can emulate adversary behaviour at scale, uncover verified attack paths, and provide evidence of impact so organisations can continuously find, fix and verify exposure.
09:40	FIRESIDE CHAT: Cybersecurity at a tipping point – the future of the security stack Simon Brady , Event Chairman (Moderator); Ulf Larsson , Security CTO, SEB - AI and the widening vendor gap: Are the largest security platforms pulling away, and can smaller vendors keep pace with the speed and investment AI demands? - Rethinking the security stack: Are banks and large organisations moving from best-of-breed point solutions towards fewer, broader platforms? Are we at a genuine tipping point? - How large organisations buy security technology today: What matters when evaluating new technology: innovation, integration, resilience, cost and vendor longevity? - What wins next: In an AI-driven world, where will specialist vendors still have an edge, and what will the security stack of the future look like?
10:05	Zero Trust controls at the endpoint John McNamee , Sales Manager, 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.

Agenda

10:10	Education Seminars Session 1	
	BeyondTrust Closing the identity blind spots across human, machines, and AI Rachel Eldridge , Solutions Engineer, BeyondTrust	Netskope See it, control it, trust it: Mastering context in a cloud-first world Lars Liljeroth , Solutions Engineer, Netskope
10:50	Networking break	
11:20	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.	
11:40	Identity in the age of agents	
	Chris Dearden , Lead Sales Engineer, Delinea - Every insider threat programme ever built assumes intent. AI agents have none – and they are already inside your environment, running on credentials nobody deliberately issued them. - This session works through three real incidents: an agent that deleted a database in a development environment; one that deleted a production environment at a major cloud provider; and one where models under evaluation escaped their sandbox and reached a third party's production estate. - In the third incident, it took 73 days to attribute, and the victim disclosed it before the attacker knew it was the attacker. No adversary in any of the three. No prompt injection. The only variable that moves between them is how far the credentials reached. - We will walk the full chain of controls – model guardrails, sandboxes, MCP gateways, inventory – and look honestly at what routes around each one. - We will finish on what it would take to hold a cloud-hosted agent to the same standard as one running on your own infrastructure: that it cannot reach your data at all without passing something able to say no.	
12:00	Agentic systems: Behaviours, patterns & security	
	Maria Christiansen , Head of Applied AI, TDC NET - Understand the core behaviours and patterns that define agentic systems. - Explore how agentic systems operate, interact, and make decisions in real-world environments. - Learn the key security considerations and controls for managing agentic systems safely and effectively.	
12:20	Education Seminars Session 2	
	Filigran Utilise your threat intelligence to improve your security posture, continuously! Magnus Lundgren , Sales Director Nordics, Filigran	Intel 471 Signal vs. Noise: How AI is reshaping the cybercrime landscape Philip Jacobs , Principal Intelligence Solutions Advisor, Intel 471
13:00	Lunch and networking	
14:00	Strengthening cyber-resilience through a vulnerability disclosure program	
	Martin Kofoed Høding , VP of Cybersecurity & CISO, SAS – Scandinavian Airlines - Building the foundation: Securing internal buy-in, learning from industry peers, and establishing clear governance. - Starting safe and scaling: Beginning with a controlled scope, building confidence, and progressing from VDP to bug bounty. - Shifting from risk to resilience: Embracing security researchers as partners and strengthening collaboration across the security and aviation communities.	
14:20	Assume breach in an AI threat landscape: From legacy backup to cyber-recovery	
	Nicolai Borchorst , Senior Sales Engineer, Rubrik - Assume breach in an AI threat landscape: Why traditional backup is no longer enough. - From legacy backup to a cyber-recovery toolbelt that compliments SOC, incident response, business continuity and compliance.	

Agenda

14:30	PANEL DISCUSSION	Beyond compliance – building cyber-resilience that actually works
	Simon Brady, Event Chairman (Moderator); Jan Jans, Legal Counsel, Finanstilsynet (Danish Financial Supervisory Authority); Marcus Mølleskov, Chief Risk & Compliance Officer, Januar; Ann-Sophie Barrington, CISO, JP/Politikens Hus; Martin Kofoed Høding, VP of Cybersecurity & CISO, SAS – Scandinavian Airlines • 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?	
15:00	Education Seminars Session 3	
	Cato Networks I am the reason you need AI security Robin Johns, WW AI Security SME, Cato Networks	Zenity Guardrails and governance strike back: The most used, most abused words in the galaxy Ben Hanson, Field CSO, Zenity
15:40	Afternoon break and networking	
16:00	PANEL DISCUSSION	The corporate security case for AI sovereignty
	Simon Brady, Event Chairman (Moderator); Laurits Ketscher, Data Protection Officer, Danish Ministry of Finance; Thomas B. Zuliani, Senior Director, Global IT Security Services, GEA Group; Maria Christiansen, Head of Applied AI, TDC NET; Tom John Fischer Jensen, Head of Privacy & Security, Semler Gruppen • 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?	
16:30	Closing remarks and end of conference	

Education Seminars

BeyondTrust

Closing the identity blind spots across human, machines, and AI

Rachel Eldridge, Solutions Engineer, BeyondTrust

Identity is the new battleground, and organisations have made real progress securing human credentials. Yet a critical blind spot remains: machine identities and AI agents.

Machine identities now outnumber humans by orders of magnitude. They're always on, rarely reviewed, and accumulate privilege silently – and AI agents are accelerating the problem. Autonomous and often over-permissioned, AI agents silently inherit the full permissions of the signed-in users and operate undetected across environment boundaries, mainly because organisations operate in silos and stack point solutions instead of building a coherent model.

Attendees will learn:

- This session cuts through the AI hype and makes the case for a holistic privilege-centric identity security approach applied consistently across human, machine, and agentic AI identities.
- You'll come away with practical ways to break down identity silos, get rid of blind spots, and give your security team the visibility and control they need to protect every identity and every privilege, wherever it lives.

Cato Networks

I am the reason you need AI security

Robin Johns, WW AI Security SME, Cato Networks

AI introduces significant security risks – but how exactly are threat actors exploiting this new attack surface? In this session, Robin Johns shares his approach to AI security from a practitioner's perspective. Drawing on his experience integrating AI into real business workflows, he explores the risks he has accepted, the challenges he has faced, and how he has overcome them.

Attendees will learn:

- How threat actors are exploiting AI as a new attack surface.
- A practitioner's approach to AI security, grounded in real-world experience.
- How Robin has integrated AI into actual business workflows.
- The security risks he has accepted along the way and how he has addressed them.

Filigran

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

Magnus Lundgren, Sales Director Nordics, Filigran

How good is your cyber-defence, and how do you know? By centralising threat intelligence from OSINT, feeds, and internal detections into one correlated view of the threats that matter to you, you can bring threat intel and detection teams closer, convert that intelligence into adversary emulation scenarios, test against relevant TTPs, and continuously validate detection and response controls against real attack techniques. This puts threat intel and detection teams on the same workflow.

Attendees will learn:

- How to centralise threat intelligence into one correlated view of the threats that matter to you.
- How to convert threat intelligence into adversary emulation scenarios and test against relevant TTPs.
- How to continuously validate detection and response controls against real attack techniques.
- How to bring threat intel and detection teams closer by putting them on the same workflow.

Education Seminars

Intel 471**Signal vs. Noise: How AI is reshaping the cybercrime landscape**

Philip Jacobs, Principal Intelligence Solutions Advisor, Intel 471

This seminar will explore how threat actors are using AI and what it is changing across the cybercrime ecosystem, while providing a reality check on what has actually changed in the attacks being seen and what is still hype. It will look at real-world deepfake incidents, how they unfolded and the lessons learned, as well as AI-enabled attacks, from AI-generated phishing and faster malware development to prompt injection and data poisoning – and whether you would know if you had been hit. It will also examine the emerging threats reshaping security priorities today.

Attendees will learn:

- How threat actors are using AI and what it is changing across the cybercrime ecosystem.
- What has actually changed in the attacks being seen, and what is still hype.
- How real-world deepfake and AI-enabled attacks unfold, and the lessons learned.
- Which emerging threats are reshaping security priorities today

Netskope**See it, control it, trust it: Mastering context in a cloud-first world**

Lars Liljeroth, Solutions Engineer, Netskope

The perimeter is dead, but your data is more active than ever. As organisations sprint toward SaaS and AI-native workflows, the security 'blind spot' isn't just growing – it's becoming the new infrastructure. True Zero Trust isn't about rigid boundaries; it's about contextual intelligence. Drawing from Netskope's unique vantage point across billions of global cloud transactions, this session explores why traditional controls fail in the face of autonomous AI agents and complex SaaS ecosystems.

Attendees will learn:

- The AI/SaaS reality: Why 'Shadow IT' has evolved into a web of autonomous agents and third-party integrations.
- Context as currency: How to transform static policies into real-time, data-aware security.
- Risk intelligence: Identifying the hidden risks within your cloud supply chain before they escalate.

Zenity**Guardrails and governance strike back: The most used, most abused words in the galaxy**

Ben Hanson, Field CSO, Zenity

An AI agent can stay within every permission, touch only allowed data, pass every security checkpoint, and still cause harm. Yet most agentic guardrail and governance conversations focus on whether an individual action is permitted. That can leave security teams with green dashboards but no answer to the more important questions: it might be allowed, but is the agent's behaviour still appropriate? Is risk emerging across the execution in a way that is invisible to our existing controls?

Attendees will learn:

- A simple mental scaffold for cutting through the noise, built around two anchors: Can vs. Should and Point-in-Time vs. the Chain.
- How Can vs. Should asks whether an agent's next action still makes sense given its goal, prior behaviour, and accumulated context, not simply whether it has permission.
- How Point-in-Time vs. the Chain shows that risk can emerge across a sequence of individually reasonable actions, even when every isolated check passes.
- Why these distinctions shape what organisations buy and prioritise, the kinds of controls that are needed, and whether anyone will be able to spot a dangerous turn in time to intervene.
- How to precisely question claims of 'governance' and guardrail effectiveness, with the information needed to build more effective architectures.