C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

Cybersecurity Think Tank

SPEAKERS



Nicolas Gomez
VP, CISO & Head of Information Security
Volvo Group



Lars Brunsgard
CISO & Sr. Director, IT Infrastructure & Operations
Topsoe



Sebastian Mabillon
Chief Information Security Officer
Bunker Holding



Sabna Sainudeen
Global Director, Application Security
Carlsberg Group



Frederik Braun
Cyber Assurance Manager
INGKA GROUP IKEA



Rune Abrahamsson
Chief Developer, Technology Enablement
Nykredit

Click Here to Register

April 15, 2027

Central European Time

Registration	**8:30 AM-9:00 AM**
Morning Networking	**9:00 AM-9:30 AM**

Opening Remarks

9:30 AM-9:40 AM

VISION VOICES KEYNOTE

9:40 AM-10:05 AM

29 Minutes in Copenhagen. Who Gets to Act Before the Attacker Does?

The average attacker now moves from a first foothold to the rest of the network in about 29 minutes. Copenhagen knows better than most what that kind of speed can do, after a single piece of malware in 2017 brought one of the world's largest shipping networks to a standstill. Yet in many organizations the decision to isolate a system, cut a supplier connection or take a revenue platform offline still waits for a meeting and an executive who may be on a plane.
This opening keynote looks at the human side of speed. Who holds the authority to act in the first half hour, what they are allowed to break without asking, and how leading CISOs agree those decision rights with the CEO, the business and the board long before the night they are needed. The fastest response, it turns out, is the decision that was already made.

PANEL

10:10 AM-10:55 AM

From Harbor to Turbine. Securing the Ships, Ports and Wind Farms That Power the North.

Few regions depend on connected infrastructure the way the Nordics do. Container ships, ports, offshore wind farms, district heating and power grids now run on software, sensors and remote access, much of it designed long before anyone imagined an attacker on the other end. A breach here does not just expose data. It can stop a vessel, quiet a wind farm or leave a city without heat in the middle of winter.
This panel brings together security leaders from shipping, energy and utilities to compare how they protect operational technology at sea and on land. How they gain visibility into equipment spread across oceans and coastlines, manage suppliers who need remote access, and keep operating safely when systems have to be taken offline.

Coffee Break

10:55 AM-11:15 AM

VISION VOICES

11:15 AM-11:30 AM

The Browser Grew Hands. What Nordic Teams Should Know Before AI Starts Clicking, Typing and Buying.

The browser used to be a window. Now it is becoming a worker. AI browsers and assistants can read a page, fill in a form, approve a request and complete a purchase on someone's behalf, and a single hidden instruction tucked inside a web page can redirect all of it. In fifteen focused minutes, this session explains why the browser has become one of the most important places to defend, what prompt injection looks like when it meets real credentials, and which simple policies let your people enjoy the help without handing the keys to whoever wrote the page.

PANEL

11:35 AM-12:20 PM

One Incident, Many Rulebooks. Making NIS2, DORA and the Cyber Resilience Act Work as One.

European security leaders are living through a remarkable convergence. NIS2, DORA and the Cyber Resilience Act each bring their own reporting clocks, supervisory expectations and personal accountability, and national versions of NIS2 differ from one country to the next. A single serious incident can now trigger duties under several regimes at once, and while Brussels has promised to simplify the reporting maze, the work of being ready cannot wait.
This panel brings CISOs from regulated sectors together to compare notes. How they fold overlapping duties into one playbook, what supervisors are actually asking for, and how to turn compliance effort into genuine resilience rather than a mountain of paperwork.

Lunch

12:20 PM-1:20 PM

VISION VOICES

1:25 PM-1:45 PM

Think Like the Attacker. Why Nordic Security Leaders Are Investing in Offense Again.

For a long time, offensive security meant the annual penetration test, a thick report and a list of findings that was already out of date by the time anyone read it. In the Nordics the regulators have noticed, with Denmark's own threat intelligence based red teaming framework for the financial sector and the threat led penetration testing DORA now requires of many financial firms. At the same time AI has changed the economics on both sides. The tools attackers use to probe your defenses around the clock are now in your hands too, and security leaders are investing in offense again with real urgency.
This session explores continuous, AI assisted red teaming. What it finds that traditional testing misses, how to run it safely against live systems, and how to turn a constant stream of findings into fixes instead of fatigue.

DISRUPTOR

1:50 PM-2:05 PM

Who Built Your AI? Mapping the New Supply Chain Behind Nordic Enterprises.

Third party risk used to mean vendors, contractors and the software they shipped. Today it also means the foundation models you call, the open weights your developers download, the plugins and connectors your agents rely on, and the data those models learned from. Each one is a link in a chain you did not forge yourself.
This disruptor session maps the new AI supply chain and shows how to inventory it, assess it and set sensible guardrails without bringing innovation to a halt.

PANEL

2:10 PM-2:55 PM

Connected to Everywhere. When World Events Reach Nordic Networks.

Nordic companies are small at home and global by nature. Teams, suppliers, data centers and customers spread across the world, and the region itself is linked by cables that run beneath the sea. A regional outage, damage to a subsea cable, a disruption at a key supplier, a sudden change in data rules or a wave of attacks aimed at one industry can travel across borders and arrive in your logs before the morning news has caught up.
This panel helps security leaders see further. How to build threat intelligence that reflects where you actually operate, how to plan for the loss of a key supplier or region, and how to brief a board that wants to understand global risk in plain business terms. It is a conversation about preparation, so your organization is never the last to know.

Networking Break

2:55 PM-3:15 PM

VISION VOICES

3:15 PM-3:30 PM

Built Secure or Not Sold. What the Cyber Resilience Act Means for Nordic Products.

For decades, the cost of insecure software landed on the customer. You bought it, you patched it, you lived with the consequences. That bargain is shifting. New rules, led by Europe's Cyber Resilience Act, are pushing responsibility back toward the people who build the products, with reporting duties, minimum standards and real penalties attached.
This session explores what secure by design means once it stops being a promise and becomes a contract term. What to demand from your vendors, what changes for the software you build yourself, and how to use this moment to finally raise the floor for everyone.

FIRESIDE CHAT

3:35 PM-4:10 PM

What I Wish I Had Known. Security Leaders on the Decisions That Shaped Them.

Every CISO carries a private library of moments. The breach that taught humility, the board meeting that changed how they speak, the hire that transformed a team, the warning they ignored once and never again. These stories rarely make it onto conference slides, yet they are where real wisdom lives.
This closing fireside invites seasoned security leaders to open that library. Honest, warm and practical, it is the conversation you usually only have late at night after an event, offered here to everyone in the room, especially those still writing the first chapters of their own careers.

Closing Remarks & Raffle Giveaway

4:10 PM-4:20 PM

Cocktail Reception

4:20 PM-5:30 PM

PARTNERS

We are currently accepting partnership opportunities for this event.