

Post event report



The 7th e-Crime & Cybersecurity Nordics

24th May 2022 | Stockholm

Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsors



“ I think you raised the bar this year in terms of presenters, topics and open panels. I enjoyed the presentations and found a lot of useful information during the day. Did a lot of networking especially with the vendors, which seemed to be perfectly aligned with current security needs, so I have already booked a follow up meeting with a few of them. Overall, a great event and great organisation; looking forward to next year’s conference. ”
Head of Information Security and Risk Management,
Qlira

“ I thoroughly enjoyed the e-Crime Congress Nordics. The content covered a range of relevant issues, with actionable information and excellent networking opportunities. A very well organised event and well worth attending. ”
CISO,
Modern Times Group

“ I have to congratulate you, your colleagues and the speakers for a very interesting congress. This was really worth my time and I got both new insights and new contacts within the business community. ”
Senior Internal Auditor,
Swedish Defense Materiel Administration

Inside this report:

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



Speakers

- Durval Batista, Regional Manager, **LastPass**
- Daniel Brett, CSO and Co-founder, **CounterCraft**
- Trevor Dearing, Director of Critical Infrastructure Solutions, **Illumio**
- Lena Stenberg Domeij, Director of Compliance, **Bank of China (Europe) S.A**
- Sebastian Engström, Regional Sales Director, Nordics, **Hunters**
- Sofia Staaf Frederiksen, Chief Information Security Officer, **Apoteket AB**
- Teppo Halonen, Regional Director Northern Europe, **Vectra AI**
- Mads Syska Hasling, Chief Information Security Officer (CISO) & Head of Financial Crime Prevention, **Saxo Bank**
- Jonas Hedquist, **Commax Sweden**
- Adam Hellstrom, Territory Account Manager, **Lookout**
- Fredrik Hertz (Moderator), Financial Services Cybersecurity Lead, Consulting, **EY Sweden**
- Magnus Jacobson, Cyber Security Senior Adviser, **Swedish Bankers' Association (SBA)**
- Emma Johansson, Senior Security Advisor, **Swedenergy**
- Bjorn Jöhren, CISO, **Max Matthiessen AB**
- Jason Kent, Hacker in Residence, **Cequence Security**
- Vijay Kishnani, Lead Cyber Security Engineer, **CybelAngel**
- Georgios Kryparos, CISO, **Einride**
- Cher Lingord, TI Analyst and SE, **Cybersixgill**
- Frederik Malmstrom, Head of Group Information Security and Data Privacy, **Handelsbanken**
- Elin Ryrfeldt, CISO, **Axfood**
- Alain Salesse, Senior Sales Engineer, **Cofense**
- Antje Schütt, Group IT Security Officer, **Vattenfall Group**
- Linnea Skärdin, Cyber Technology Specialist, **Darktrace**
- Dimitrios Stergiou, Group Chief Information Security Officer, **Trustly Group AB**
- Navaz Sumar, CISO, TF Bank
- Martin Szabo, Sales Director Nordics & Benelux, **Synack**
- Sachin Thombre, Senior Cybersecurity Solutions Specialist, **Imperva**
- Matthew West, Solutions Architect Benelux and Nordics, **Synack**
- Jan Willekens, Head of Cyber Defense Center, **Ericsson**

Key themes

- Closing the cybersecurity skills gap
- Securing the citizen
- From smart machines to smart cities – securing the IoT
- Moving to Cloud Native
- Are AI/ML solutions the answer or just hype?
- Securing digital currencies
- Is ransomware the canary in the coal mine?
- Behavioural analytics
- Re-engineering the SOC: from logs to automated XDR
- Building better Cloud security
- Building-in security from DevOps to SecDevOps
- Can zero trust be done?

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

Agenda			
08:00	Registration and networking break		
08:50	Chairman's welcome		
09:00	<p>Cost, agility and completeness; what to sacrifice when building a modern vulnerability management programme</p> <p>Georgios Kryparos, CISO, Einride</p> <ul style="list-style-type: none"> • How broad is the scope of vulnerability management in a modern enterprise? • Where to start and how? • Which areas will give you the most bang for the buck? • How to unify all the information in 1 dashboard and make it concrete and actionable? 		
09:20	<p>APIs as your ultimate honeypot</p> <p>Sachin Thombre, Senior Cybersecurity Solutions Specialist, Imperva</p> <ul style="list-style-type: none"> • How the use of the accelerator of all modern web applications goes horribly wrong, and what to do to prevent it • What are some of the popular API security measures and why they are not enough • How to recognise data leakages and what to do to counter them • How to spot irregular behaviour in both B2B and B2C APIs 		
09:40	<p>Do you know what information your APIs are leaking?</p> <p>Jason Kent, Hacker in Residence, Cequence Security</p> <p>Attend this session to fully understand the API security risks your organisation faces. Topics include:</p> <ul style="list-style-type: none"> • Security risks associated with the increased use of health monitoring APIs, API specifications, and GraphQL • Compliance and governance risks related to APIs that may inadvertently expose sensitive data • Why APIs used to facilitate account login/registration and inventory lookups are more susceptible to automated attacks 		
10:00	<p>Combatting financial crime in the digital age</p> <p>Mads Syska Hasling, Chief Information Security Officer (CISO) & Head of Financial Crime Prevention, Saxo Bank</p> <ul style="list-style-type: none"> • Breaking down silos to ensure best in class capabilities (tactical and strategic) to identify, prevent, detect and respond to the growing threat of cybercrime • Benefits of joining our people, processes and technology within Cyber, Fraud, AML and MAR Surveillance teams under one department • Lessons learnt from the ongoing cyber-journey at Saxo Bank 		
10:20	<p>Education Seminars Session 1</p> <table border="1"> <tr> <td> <p>Cybersixgill A day in the life of a hacker Cher Lingord, TI Analyst and SE, Cybersixgill</p> </td> <td> <p>Synack Harness the crowd: It's your best chance of finding every vulnerability that matters Martin Szabo, Sales Director Nordics & Benelux, and Matthew West, Solutions Architect Benelux and Nordics, Synack</p> </td> </tr> </table>	<p>Cybersixgill A day in the life of a hacker Cher Lingord, TI Analyst and SE, Cybersixgill</p>	<p>Synack Harness the crowd: It's your best chance of finding every vulnerability that matters Martin Szabo, Sales Director Nordics & Benelux, and Matthew West, Solutions Architect Benelux and Nordics, Synack</p>
<p>Cybersixgill A day in the life of a hacker Cher Lingord, TI Analyst and SE, Cybersixgill</p>	<p>Synack Harness the crowd: It's your best chance of finding every vulnerability that matters Martin Szabo, Sales Director Nordics & Benelux, and Matthew West, Solutions Architect Benelux and Nordics, Synack</p>		
11:00	Networking break		
11:30	<p>EXECUTIVE PANEL DISCUSSION Financial institutions</p> <p>Magnus Jacobson (Moderator), Cyber Security Senior Adviser, Swedish Bankers' Association (SBA); Lena Stenberg Domeij, Director of Compliance, Bank of China (Europe) S.A; Frederik Malmstrom, Head of Group Information Security and Data Privacy, Handelsbanken; Mads Syska Hasling, CISO & Head of Financial Crime Prevention, Saxo Bank; Navaz Sumar, CISO, TF Bank</p> <ul style="list-style-type: none"> • What are the most worrying threats you see against financial institutions? • How do new resilience regulations help in the battle against cybercriminals? • Does cybersecurity fit naturally into the three lines of defence model? • How secure are the market infrastructures upon which the financial institutions rely (e.g. payment systems like SWIFT or Fedwire or CHAPs or even central banks)? 		
11:50	<p>Fast and furious attacks: Using AI to surgically respond</p> <p>Linnea Skärdin, Cyber Technology Specialist, Darktrace</p> <ul style="list-style-type: none"> • Today's cybersecurity teams are overwhelmed; threats are simply spreading too quickly • The rear-view approach is no longer enough • Autonomous response uses self-learning AI to effectively contain and combat a cyber-attack • Darktrace protects entire digital ecosystems and equips security teams for the future • Learn about key threat finds: Sodinokibi and Log4Shell 		
12:10	<p>Secure the digital front doors of your organisation and the sensitive data inside</p> <p>Adam Hellstrom, Territory Account Manager, Lookout</p> <ul style="list-style-type: none"> • Modernise secure web access with a zero trust approach • Transform secure connectivity to private apps in your data centre and public cloud • Gain visibility & control, and protect your data as you enable SaaS apps • Secure the endpoints you use the most 		

Agenda

12:30	How to make your SOC run more effectively in 2022	
	<p>Sebastian Engström, Regional Sales Director, Nordics, Hunters</p> <p>The shift to the cloud and the extension of the attack surface requires new approaches for threat detection and response. During this session, you'll learn:</p> <ul style="list-style-type: none"> • The definition of a SOC Platform and how it can help security teams • Strategies to empower your security team mitigate real threats faster and more reliably than SIEMs to incidents that matter across the attack surface • How Fortune 1000 companies are using Hunters' SOC Platform to ingest, cross-correlate, prioritise and investigate incidents 	
12:50	Education Seminars Session 2	
	<p>Cofense Implementing an adaptive email security architecture with Cofense Alain Salesse, Senior Sales Engineer, Cofense</p>	<p>CybelAngel Finding the leaky data links in your supply chains – data security beyond perimeters Vijay Kishnani, Lead Cyber Security Engineer, CybelAngel</p>
13:30	Lunch and networking break	
14:30	EXECUTIVE PANEL DISCUSSION Priorities for 2022/23	
	<p>Dimitrios Stergiou (Moderator), CISO, Trustly; Sofia Staaf Frederiksen, Chief Information Security Officer, Apoteket AB; Bjorn Johren, CISO, Max Matthiessen AB; Emma Johansson, Senior Security Advisor, Swedenergy; Antje Schütt, Group IT Security Officer, Vattenfall Group</p> <ul style="list-style-type: none"> • Data privacy or security? How will companies view 'security' in the post-pandemic world? • Hybrid working: problem solved, or problem postponed? • The issue of 'basic' cyber-hygiene (or 'why can't we stop ransomware?') • Is 2022 the year of Cloud? And have the security implications of Cloud been exaggerated? 	
14:50	The power of deception tech: Uncovering Russian TTPs targeting Ukrainian infrastructure	
	<p>Daniel Brett, CSO and Co-founder, CounterCraft</p> <ul style="list-style-type: none"> • How our deception environments uncovered a February attack involving threat actors attempting to attack Ukrainian government infrastructure; an in-depth analysis of this attack, how it was discovered, and the intel gathered • The importance of being prepared for cyber-warfare on the back of global events • Takeaways for the financial sector and critical infrastructure 	
15:10	CIO Forum Cyber Security 2022	
	<p>Durval Batista, Regional Manager, LastPass, and Jonas Hedquist, Commax Sweden</p> <ul style="list-style-type: none"> • Security risks associated with poor password hygiene at the workplace • Passwords are one of the weakest links in the cybersecurity chain – what actions should business take to improve this? • Benefits of implementing an organisation-wide Password Manager 	
15:30	Education Seminars Session 3	
	<p>Illumio How isolation stops the spread of ransomware Trevor Dearing, Director of Critical Infrastructure Solutions, Illumio</p>	<p>Vectra AI Detecting threat actors that others miss – real world examples Teppo Halonen, Regional Director Northern Europe, Vectra AI</p>
16:10	Networking break	
16:30	EXECUTIVE PANEL DISCUSSION Regulation	
	<p>Fredrik Hertz (Moderator), Financial Services Cybersecurity Lead, Consulting, EY Sweden; Elin Ryrfeldt, CISO, Axfood; Jan Willekens, Head of Cyber Defense Center, Ericsson; Magnus Jacobson, Cyber Security Senior Adviser, Swedish Bankers' Association (SBA)</p> <ul style="list-style-type: none"> • What is the global regulatory direction? Do we see a pattern across sectors? • We all assume resilience is key for service providers. Do we need regulations? • How far should companies plan for disruption? When does it become someone else's problem? • What are the evolving operational models for resilience? How can we integrate different competencies? 	
16:50	Does cybersecurity fit naturally into the three lines of defence model?	
	<p>Navaz Sumar, CISO, TF Bank</p> <ul style="list-style-type: none"> • How to tackle cyber-risks in 3LoD • To whom should you report cybersecurity risk • How do you communicate cybersecurity and risks • The convergence of operational risk and cybersecurity 	
17:10	Third-party risk: Governance, monitoring, auditing	
	<p>Dimitrios Stergiou, Group Chief Information Security Officer, Trustly Group AB</p> <ul style="list-style-type: none"> • Third party everywhere: Third-party components that make me lose sleep • Assuming control: How we approach the cloud services monster • Conclusions 	
17:30	Conference close	

Education Seminars	
<p>Cofense</p> <p>Implementing an adaptive email security architecture with Cofense</p> <p>Alain Salesse, Senior Sales Engineer, Cofense</p>	<p>What is an adaptive security architecture and what are the objectives? With so much focus on cyber-attack prevention, many security teams have adopted an incident response mindset versus one that assumes systems are compromised and require continuous monitoring and remediation.</p> <p>We'll walk you through the benefits and objectives of implementing an adaptive security architecture and risk framework.</p> <p>The current situation in email and phishing security – We'll share some of the latest insights from the industry and what we're seeing through our unique combination of artificial, human, and high-fidelity intelligence.</p> <p>Implementing adaptive security architecture and risk framework with Cofense – We'll talk through how to classify your existing and potential email security investments to increase your security posture while reducing costs, vendors, and configuration complexity.</p>
<p>CybelAngel</p> <p>Finding the leaky data links in your supply chains – data security beyond perimeters</p> <p>Vijay Kishnani, Lead Cyber Security Engineer, CybelAngel</p>	<p>Ask yourself, where is the risk in sharing data with third parties? Is the risk the third party, or is the risk having your data leak? The real danger is the data leak! The leak being at a third party just makes it more challenging to locate. Instead of making third parties jump through long and sometimes unproductive audits, a new perspective is needed a data risk first approach.</p> <p>A data risk first approach focuses on locating whatever data matches your organisation's regardless of where it appears. By focusing on which data matches, you gain visibility and protection far beyond a company's perimeter into third, fourth, and fifth parties. This increase in visibility frees cybersecurity teams from choosing which partners get monitoring.</p> <p>You will learn:</p> <ul style="list-style-type: none"> • Why your risk is with the data, not third parties • What is a data risk first approach? • How DRPS tools can assist in a data risk first approach
<p>Cybersixgill</p> <p>A day in the life of a hacker</p> <p>Cher Lingord, TI analyst and SE, Cybersixgill</p>	<p>Threat intelligence's value is sometimes hard to explain. By tracking the cyber kill chain, we will see how organisations can try and prevent attacks further up the killchain by having visibility into the underground.</p> <p>Join this session to learn more about:</p> <ul style="list-style-type: none"> • Common framework for analysing attacks • How CTI fits into all of this • A useful way of getting into the attacker mindset • A bit about Boris
<p>Illumio</p> <p>How isolation stops the spread of ransomware</p> <p>Trevor Dearing, Director of Critical Infrastructure Solutions, Illumio</p>	<ul style="list-style-type: none"> • See how to stop the propagation of ransomware • Identify the potential weaknesses in your infrastructure • Build a more resilient defence against future threats

<p>Synack</p> <p>Harness the crowd: It's your best chance of finding every vulnerability that matters</p> <p>Martin Szabo, Sales Director, Nordics & Benelux, and Matthew West, Solutions Architect, Benelux and Nordics, Synack</p>	<p>In today's environment, traditional pen testing is broken. Synack, fuelled by a diverse community of vetted and trusted researchers, can help you find the exploitable vulnerabilities you need to deal with.</p> <p>In this session, you will learn:</p> <ul style="list-style-type: none"> • How a crowd of ethical hackers, available on-demand and strongly incentivised to deliver results, can transform your pen testing • How Synack's coverage compares to the general market • What a typical testing engagement looks like, including scoping targets, discovering vulnerabilities, and the lifecycle of a vulnerability report, from initial submission to patch verification
<p>Vectra AI</p> <p>Detecting threat actors that others miss – real world examples</p> <p>Teppo Halonen, Regional Director Northern Europe, Vectra AI</p>	<p>The impact of the global pandemic has resulted in a paradigm shift that has drastically expanded attack surfaces, as hybrid and remote working environments become the norm.</p> <p>With cybercriminals looking for easy targets and opportunities to steal personal information, they too have adapted to find new ways in which they can exploit and bypass legacy security systems.</p> <p>During our presentation we will cover:</p> <ul style="list-style-type: none"> • How highly evasive threat actors perpetrate their attacks • Insight from some of our customers on the autonomy of the attack • How Vectra saw the attacks earlier and stopped them being breached