Post event report

Strategic Sponsors

CYLANCE

DARKTRACE

FIREMON

MICRO FOCUS

PHISHME

Recorded Future

Education Seminar Sponsors

Flowmon
Driving Network Visibility

foreseeti

SABSA COURSES.COM

Secure Link

Synack

THALES

"This was my first time at e-Crime & Cybersecurity Nordics. Although I work specifically in the fraud area, I found most of the sessions relevant and interesting. A balanced mix of more 'product marketing' sessions and pure knowledge sharing sessions with interesting topics."
Chief Product Owner, Fraud Management, Nordea

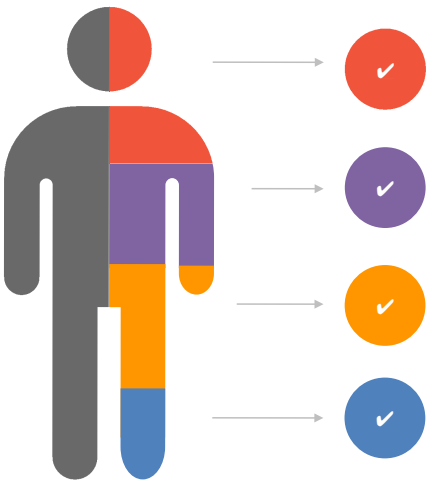
"I thoroughly enjoyed the e-Crime Congress Nordics. The content covered a range of relevant issues, with actionable information and excellent networking opportunities. A very well organised event and well worth attending."
CISO, Modern Times Group

Inside this report:

Key themes

- Is AI the answer?
- When state-actors are the main threat
- Optimising enterprise architectures
- Beating ransomware: It can be done
- Closing the door on email-delivered malware
- Secure application development
- Will your security precautions pass the scrutiny test?

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

Urmas Aamisepp,
Chief Information Security Officer
Clas Ohlson

Henrik Akerstrand,
Regional Manager for Nordics
Cylance

Richard Cassidy,
Head of Solution Engineering EMEA
Synack

John J. Czaplewski,
Director of Professional Services
David Lynas Consulting Ltd

Marcel Derksen,
Senior Sales Engineer
Thales eSecurity

Brendan Dowell,
Head of Security
Kindred Group

Eward Driehuis,
Chief Research Officer
SecureLink

Jacob Henricson,
Senior Risk Management Advisor
foreseeti

David Janson,
VP Sales, UK & Europe
PhishMe

Suzette Loubser, Account Executive
Darktrace

Göran Melvås,
Identity and Access Manager
Skandia Norden

Lars Nikamo,
Identity & Security Specialist
Micro Focus

Brian O'Toole, CISO
Ericsson

Josefine Östfeldt,
IT and Information Security Manager
Polismyndigheten

Pablo Ridgeway,
Sales Engineer EMEA
FireMon

Tomas Sarocky, Area Manager
Flowmon Networks

Dimitrios Stergiou,
Chief Information Security Officer
Modern Times Group

Staffan Truvé, Co-founder & CTO
Recorded Future

Bjørn R. Watne, CISO
Storebrand & SPP

Agenda

08:00	Registration
08:50	Chairman's welcome
09:00	**When security becomes part of the business** **Josefine Östfeldt,** IT and Information Security Manager, Polismyndigheten • Reasons why we need to be more agile • Actions taken to integrate information security into development and operations • Key factors to change how we work with IT and information security
09:20	**Is your security management solution keeping up? Threat hunting – beyond alerts and IOCs** **Pablo Ridgeway,** Sales Engineer EMEA, FireMon • Security playbook • A new perspective – assumed compromise • How security fails • A hunting paradigm • Primer on data and analytics
09:40	**How is artificial intelligence changing the way we can combat threats on clients and servers?** **Henrik Akerstrand,** Regional Manager for Nordics, Cylance • Get an introduction into why criminals have an easy time circumventing traditional endpoint defences • Learn how AI is used to predictively detect and block cyber attacks on the endpoint • Hear what impact deploying an AI driven solution can have for your organisation
10:00	**Education Seminars | Session 1**
	foreseeti **Threat modelling: The challenge in managing risk of both structural and technical vulnerabilities** **Jacob Henricson,** Senior Risk Management Advisor, foreseeti **Thales eSecurity** **GDPR: Regulation, myths and encryption** **Marcel Derksen,** Senior Sales Engineer, Thales eSecurity
10:40	Networking and refreshments break
11:10	**Password reuse attack: A simple attack raising some challenging questions** **Brendan Dowell,** Head of Security, Kindred Group • How another company's misfortune (leaked customer credentials) will become your problem • Why human nature makes this simple attack so effective • More innovative methods to detecting and protecting from password reuse attack • Dealing with indifference: The era of 'total customer responsibility' for account security is over
11:30	**The 2017 phishing threat landscape** **David Janson,** VP Sales, UK & Europe, PhishMe • High-profile leaks and mature malware tools in phishing emails and how this has led to the resurgence and emergence of ransomware and botnet malware • What is meant by the 'phishing threat landscape', how attackers have evolved this and the risks that poses to the enterprise • What your enterprise can do in the face of all this, and goals for a holistic, comprehensive and agile defence
11:50	**The Enterprise Immune System: Using machine learning for next-generation cyber defence** **Suzette Loubser,** Account Executive, Darktrace • How new machine learning and mathematics are automating advanced cyber defence • Why 100% network visibility allows you to detect threats as they happen, or before they happen • How smart prioritisation and visualisation of threats allows for better resource allocation and lower risk • Real-world examples of unknown threats detected by 'immune system' technology
12:10	**GDPR – a business enabler** **Urmas Aamisepp,** Chief Information Security Officer, Clas Ohlson • GDPR doesn't have to be a complete nightmare • Increasing customer trust in handling their data in the right way creates a positive spiral • More data leads to more insight that can generate relevant offers, creating value for customers

Agenda

12:30 — Education Seminars | Session 2

Flowmon Networks
Is an attacker hidden in your networks?
Tomas Sarocky, Area Manager, Flowmon Networks

SABSAcourses
Architecting enterprise security to deliver business value
John J. Czaplewski, Director of Professional Services, David Lynas Consulting Ltd

13:10 — Lunch and networking

14:10 — Application security in an Agile development world

Dimitrios Stergiou, Chief Information Security Officer, Modern Times Group

- Why secure application development is important
- Four approaches to secure application development that don't seem to work
- What should a secure application development programme cover?
- How to integrate secure application development with the Agile practice
- How can security help in the DevOps world?

14:30 — Identity is the new security

Lars Nikamo, Identity & Security Specialist, Micro Focus

- What is the role of identity within security
- Where to start? Don't try to eat the elephant at once
- How to prepare yourself for and to protect yourself against the insider threats

14:50 — Using AI and machine learning to close the protection deficit

Staffan Truvé, Co-founder & CTO, Recorded Future

- To properly protect themselves against cyber threats, organisations must use threat intelligence
- The volume and complexity of threats means human analysts cannot handle this alone – they need machine assistance in the form of AI and machine learning (ML)
- AI/ML can both automate the tedious task of sifting through massive amounts of information to find what is relevant, and find hidden patterns in complex data
- The successful combination of human analysts and AI/ML is what allows cyber defenders to both anticipate and defend against the ever-growing threat landscape

15:10 — Education Seminars | Session 3

SecureLink
50 shades of nasty: Past, present and future
Eward Driehuis, Chief Research Officer, SecureLink

Synack
Threat landscape evolution and automation techniques
Richard Cassidy, Head of Solution Engineering EMEA, Synack

15:50 — Networking and refreshments break

16:10 — Artificial intelligence: The new solution for IAG and the cloud

Göran Melvås, Identity and Access Manager, Skandia Norden

- How artifical intelligence in identity and access governance and identity and access management can mitigate the new risks in the cloud-based environment, where identity is the new perimeter
- Using AI in IAM can be more cost-effective and more secure
- How these can be part of an effective GDPR strategy
- Artificial intelligence in IAG and IAM: An important part of the identity base

16:30 — EXECUTIVE PANEL DISCUSSION — So, do you really need a CISO?

Urmas Aamisepp, CISO, Clas Ohlson

Brian O'Toole, CISO, Ericsson

Dimitrios Stergiou, CISO, Modern Times Group

Bjørn R. Watne, CISO, Storebrand & SPP

16:50 — Closing remarks

17:00 — Conference close

Education Seminars

Flowmon Networks

Is an attacker hidden in your networks?

Tomas Sarocky, Area Manager, Flowmon Networks

Today's security tools are focused on prevention and protection against threats and attacks. There are several tools on the market providing this solution. However, modern approach should be very different. Detection and reaction on security breaches should be the main focus of secured networks. And the best way to detect an event is to monitor what is happening in the network. Do you really know what, who, where and how its doing?

What attendees will learn:

- Why your current cybersecurity tools are not enough
- How to upscale your data security into the next level
- What you can find out in network traffic monitoring
- What are the possibilities in network monitoring
- How network monitoring and diagnostics will improve your security

foreseeti

Threat modelling: The challenge in managing risk of both structural and technical vulnerabilities

Jacob Henricson, Senior Risk Management Advisor, foreseeti AB

Companies today are experiencing and ever-increasing connectivity and complexity of infrastructure risk management. The underlying challenge today is that infrastructures are complex and interconnected, let alone the fact that a lot is run in the cloud. With the complexity of architectures increasing, the focus on technical vulnerabilities is not enough. Traditional vulnerability scanning offers insight on technical vulnerabilities but lacks the ability to prioritise what to focus on.

That said, in general, there needs to be a more holistic approach to ensure that risk is managed in a proper way related to IT infrastructures. Using a combination of technical and structural vulnerabilities, being able to map large infrastructures in a scalable way, needs to be combined with a probabilistic approach in threat modelling, which enables organisations to focus on true risk instead of theoretical risk on a technical level.

Taking this further, and being able to focus on true business risk, requires a new approach. At the Royal institute of technology, extensive research has been conducted in threat modelling and the probability of a certain set of parameters to be exploited to get access to an infrastructure. Join this seminar to learn the latest of research on threat modelling from both academia and the corporate world.

What attendees will learn:

- Distinction between technical and structural vulnerabilities
- How to address the challenges in scaling traditional risk assessments and threat modelling of complex IT infrastructures with objective fact-based data
- Using research findings to perform threat modelling on large corporate IT infrastructures
- How to use threat modelling in the design process of IT infrastructures

SABSAcourses

Architecting enterprise security to deliver business value

John J. Czaplewski, Director of Professional Services, David Lynas Consulting Ltd (SABSAcourses)

The modern enterprise requires enterprise security that demonstrably delivers true business value by enabling business goals and objectives. Today's enterprise must transform its enterprise security functions from threat-focused sources of cost and business prevention into a Center of Excellence delivering business value to enable the risk-managed pursuit of core business goals and objectives.

The SABSA Enterprise Security Architecture Framework and Methodology is used to architect security that traceably delivers business value by holistically addressing a dynamic risk environment that includes threats and opportunities. An effective ESA assures deployment of the right security, in the right place, at the right time, for the right amount of money, enabling your organisation to pursue its unique set of goals and objectives.

What attendees will learn:

- The Enterprise Security Architecture Vision
- Where to start
- How to plan and prioritise
- How to establish capability
- How to develop maturity
- How to achieve excellence

Education Seminars	
SecureLink **50 shades of nasty: Past, present and future** **Eward Driehuis,** Chief Research Officer, SecureLink	SecureLink's Research Chief shares three interconnected war stories on the underground, ransomware and geopolitical threats. He'll extrapolate their impact and risk to your organisation, give pointers on combating them with people, process & technology, and indulge in a small peek into the future. What attendees will learn: • The people, processes and technology connecting spies, criminals and nation states • Where the threat landscape is headed and what that means for your organisation • What security solutions criminals hate most
Synack **Threat landscape evolution and automation techniques** **Richard Cassidy,** Head of Solution Engineering EMEA, Synack	In today's cybercriminal world, the perception of attacker capability is vastly different from the reality of what organisations are having to defend against. Furthermore, an understanding of what attackers are after, why and how they monetise stolen or compromised assets, serves as one of the key factors in better understanding how current defences and security processes, tools and frameworks, stack up, against the latest techniques available to the cybercriminal elite. What attendees will learn: • How the three main attacks classes have evolved over the decades • What tools, techniques and procedures cybercriminals use today, with a deeper dive view of the cybercriminal economy that allows instant monetisation of stolen or compromised business assets • What the most popular tools used today are and provide insights into a concerning (but rapidly growing) trend in attacker automation, with levels of sophistication akin to the capabilities of nation state groups • How to build an effective security testing programme in response to these changing trends and capabilities by the adversary and how to disrupt the attacker • Through the employment of your own sophisticated security functions and frameworks, to help originations change the game in what has become an adversarial golden age for cybercriminals across the world
Thales eSecurity **GDPR: Regulation, myths and encryption** **Marcel Derksen,** Senior Sales Engineer, Thales eSecurity	The GDPR comes into force on 25th May 2018. A lot of information is available from a variety of sources, explaining the Regulation and its many facets. But how do you sort the real news from the fake news? Some of the available information on GDPR from certain sources is, to put it kindly, somewhat inaccurate. What attendees will learn: • What the Regulation does and does not say • What's new in terms of data protection and GDPR and what is not • An exploration to explode some myths • Review of some specific areas of GDPR where Thales might be able to help as part of an overall approach