Post event report

Strategic Sponsors

corelight

CROWDSTRIKE

DARKTRACE

ExtraHop

RANGEFORCE

SentinelOne

Education Seminar Sponsors

LexisNexis RISK SOLUTIONS

onelogin

Recorded Future

Silobreaker

Synack

tripwire

“Thank you for a conference with many great speakers and up-to-date information about the new cybersecurity arena. Listening to informative presentations from top speakers gave inspiration as well as knowledge for ways to work against e-crime. I am happy that I participated.”

Fraud and Aml Specialist, Ikano Bank

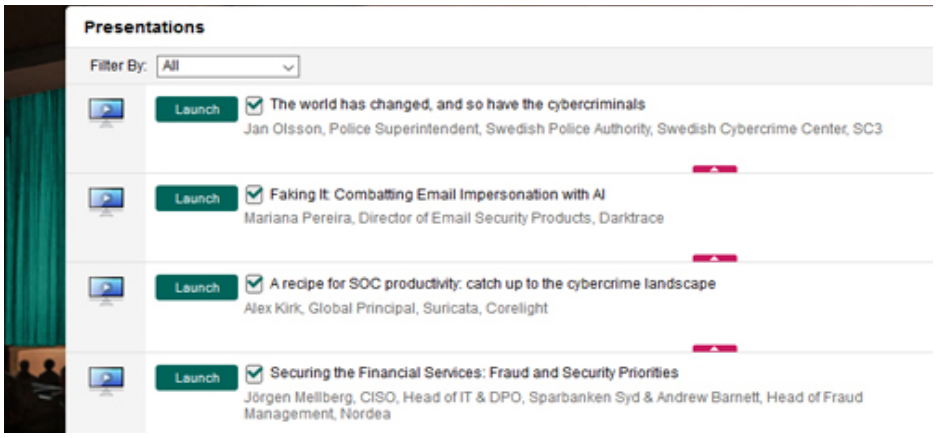
“You’ve rallied some amazing people to come speak and a very empowering group of experts that you were able to bring together on panel discussions. All sessions were very informative. All in all, a great event, packed with lots of knowledge and great speakers, offering a compact source of inspiration.”

Information Security Assurance Officer, Swedbank

“The conference went well especially as it had to be made online instead of in person due to the coronavirus pandemic. It was really well organised and the platform was easy to use. As for the presentations, it’s always valuable to hear expert opinions in the context of issues that we deal with everyday in IT/information security. There was a wide range of speakers with different backgrounds that allowed for great diversity and ensuring that all important aspects, hardships, processes are identified giving a better contextual background to the issues discussed.”

Information Security Officer, Qliro AB

Inside this report:



Key themes

- Cybersecurity for business resilience
- Rethinking identity and access management
- Securing the customer – are your websites up to it?
- Building in security: easier said than done?
- Stuck in the Cloud
- Protection versus business needs
- Performing critical security tasks remotely – how can CISOs regain control?
- Securing and protecting remote employees

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

Simon Brady, Managing Editor
AKJ Associates Ltd

Andrew Barnett,
Head of Fraud Management
Nordea

Rupert Collier,
Director of Sales – EMEA and APAC
RangeForce

Abdelkader Cornelius,
Threat Intelligence Analyst
Recorded Future

Andy Dyrcz, Head of Cyber Security
Linkfire

Terje Aleksander Fjeldvaer,
Head of Financial Cyber Crime Center
DNB

Sverker Forsberg,
Information Security Officer
Södersjukhuset

Predrag Gaikj, Head of Information Security and Risk Management
Qliro AB

Peter Granlund, CISO, If Group

Hanne Hansen, Interim CISO, Ørsted

Anthony Herring,
Head of Cyber – Nordics
Marsh

Alex Kirk, Global Principal, Suricata
Corelight

Göran Kördel, CIO, Boliden Group

Max Mansson, Client Director
Silobreaker

Jörgen Mellberg,
CISO, Head of IT & DPO
Sparbanken Syd

Jamie Moles, Senior Security Engineer
ExtraHop

Paul Norris, Senior Sales Engineer
Tripwire

Jan Olsson, Police Superintendent,
Swedish Police Authority,
Swedish Cybercrime Center
SC3

Mariana Pereira,
Director of Email Security Products
Darktrace

Ronald Pool, Senior Solutions Engineer
CrowdStrike

Stuart Sharp, VP of Solution Engineering
OneLogin

Sebastian Claydon Takle,
Subject Lead – Threat Intelligence for Financial Cyber Crime Center
DNB

Jan Tietze,
Director Security Strategy EMEA
SentinelOne

Rijk Vonk,
Regional Director Benelux & Nordics
Synack

Agenda

08:00 Login and networking

08:55 Chairman's welcome

09:00 **BEC attacks: forward-thinking defence strategies for the most financially damaging cybercrime**

Terje Aleksander Fjeldvaer, Head of Financial Cyber Crime Center, and **Sebastian Claydon Takle,** Subject Lead – Threat Intelligence for Financial Cyber Crime Center, DNB

- Business email compromise attacks: fraudsters are constantly evolving and the price and sophistication of attacks are more damaging than ever
- Case studies from the Financial Cyber Crime Center at DNB on the current state of business email compromise
- Analysis of the current threat landscape and strategies for defence and risk mitigation

09:20 **Talking to the board: the new realities of IT security**

Jamie Moles, Senior Security Engineer, ExtraHop

- The large-scale adoption of work-from-home technologies, heightened activity on customer-facing networks, and greater use of online services has greatly increased the risk of misconfigurations and cyber-threats
- Hackers have taken advantage of these new vulnerabilities and in recent weeks, ransomware attacks have affected several major organisations
- When attacks like these make headlines, board members have one question for CISOs: how can we be sure that won't happen to us?
- Join to hear top strategies for CISOs to lead board-level conversations about risk management amidst the stark new realities of IT

09:40 **Reducing time to containment: THE security priority**

Jan Tietze, Director Security Strategy EMEA, SentinelOne

With limited resources, an ever-growing skills gap and an escalating volume of security alerts, organisations are left vulnerable to what is perceived to be unavoidable risk. This environment is demanding more of already resource-constrained CISOs. In this keynote we will be discussing how automation can help to:

- Drastically reduce the amount of uninvestigated and unresolved alerts
- Automate time-consuming investigations and remediate well-known threats
- Act as a force multiplier for resource-constrained security teams

10:00 **EXECUTIVE PANEL DISCUSSION** **Preparing for the new normal: business continuity and cybersecurity**

Up until a few months ago, it was unimaginable that entire workforces would be operating remotely. The COVID-19 crisis was a real test of organisations' business continuity plans. One particular challenge for businesses was ensuring cybersecurity was properly considered, and their critical systems and data remain protected. How have cybersecurity teams adapted to a changing business environment?

Peter Granlund, CISO, If Group

Sverker Forsberg, Information Security Officer, Södersjukhuset

10:20 **Education Seminars | Session 1**

OneLogin	Tripwire
Empower your employees to work securely and efficiently from home	**Securing cloud environments, staying on top of cloud configurations to prevent data leaks and inadvertent exposure**
Stuart Sharp, VP of Solution Engineering, OneLogin	**Paul Norris,** Senior Sales Engineer, Tripwire

10:50 Networking break

11:20 **Cybersecurity risks in the manufacturing industry: How are the cyber-insurers adapting?**

Anthony Herring, Head of Cyber – Nordics, Marsh

- 'Debunking' the myths of the cyber-insurance market
- Overview of loss trends in the Nordics region
- Current challenges for the manufacturing industry and the insurance market, including:
  - The convergence of IT and OT
  - Managing your supply chain
  - Physical damage triggered by cyber-events
  - Cyberwarfare and geopolitical tensions

11:40 **Upskilling security teams through cyber-simulation**

Rupert Collier, Director of Sales – EMEA and APAC, RangeForce

- Exposing teams safely to real threats to help prepare for an actual attack is a smart way to build cyber-resilience
- See how simulation-based training elevates cyber-skills, bridges staffing gaps, and improves detection, containment, and remediation of cyber-attacks
- Get real evidence of how cutting edge training helps overcome limited budgets and time, as well as train in place requirements
- See the cyber-simulation platform in action and learn how it can help you develop customised training regardless of team size or skills

Agenda

12:30 — Hacking exposed

Ronald Pool, Senior Solutions Engineer, CrowdStrike

- An in-depth look at the speed of modern-day hacking tactics & techniques
- Join us to observe new attack techniques based on our renowned threat landscape, to defeat ransomware, spear phishing attacks and malware-free intrusions
- Having the ambition to not pay ransomware is great, but is it feasible? Can you handle the infection alone or do you need specialised help? And what are the hidden costs even if you do pay?
- Learn why security hygiene matters and how partnering can help solve the skills shortage in your security team. We will present new tips & tricks to improve your organisation's time to respond

12:20 — Education Seminars | Session 2

Recorded Future	Synack
You get what you pay for – pricing on the Nordic underground economy	**Can't change the cybersecurity game? Change its structure**
Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future	**Rijk Vonk,** Regional Director Benelux & Nordics, Synack

12:50 — Lunch and networking break

13:50 — The world has changed, and so have the cybercriminals

Jan Olsson, Police Superintendent, Swedish Police Authority, Swedish Cybercrime Center, SC3

- Insights on how cybercrime has changed in the new normal and methods in which criminals have exploited the crisis
- Overall, fraud cases are down – how do we ensure they continue to decrease and how organisations can avoid getting victimised
- Learnings from recent data breaches in the Nordics region on the evolving tactics of cybercriminals
- Why collaboration between law enforcement and industry is critical to successfully tackling cybercrime

14:10 — Faking it: combatting email impersonation with AI

Mariana Pereira, Director of Email Security Products, Darktrace

- Today, 94% of cyber-threats still originate in the inbox. 'Impersonation attacks' are on the rise, as AI is increasingly being used to automatically generate spear-phishing emails, or 'digital fakes' that expertly mimic the writing style of trusted contacts and colleagues
- Humans can no longer distinguish real from fake on their own, so businesses are increasingly turning to AI to distinguish friend from foe and fight back with autonomous response
- In an era when thousands of documents can be encrypted in minutes, learn how 'immune system' technology can take action in seconds and stop cyber-threats before damage is done

14:30 — A recipe for SOC productivity: tools and process to help you catch up to the cybercrime landscape

Alex Kirk, Global Principal, Suricata, Corelight

- Lots of people, especially at conferences like these, talk about tracking specific adversaries
- But most of them are only reacting to alerts about adversary activity, not proactively tracking them, because they're already overwhelmed
- See how integrated detection and metadata lets you accelerate/automate your IR enough to have a chance of catching up to bad actors

14:50 — EXECUTIVE PANEL DISCUSSION — Securing the financial services: fraud and security priorities

At the onset of 2020, security teams in the financial services tackled a set of intertwined problems; heavy regulatory demands; the inefficiency of legacy systems that seemed posed against digitisation; higher reliance on remote banking services; third-party risk in the supply chain; the heavy appeal financial institutions have for would-be hackers and malicious insiders. The COVID-19 crisis has exasperated old challenges and manifested new problems. How have financial institutions adapted to this new environment to mitigate the ever-increasing cybersecurity risks and protect their organisation and customers?

Jörgen Mellberg, CISO, Head of IT & DPO, Sparbanken Syd; **Andrew Barnett,** Head of Fraud Management, Nordea

15:10 — Education Seminars | Session 3

Silobreaker

Monitoring threats to areas of operation

Max Mansson, Client Director, Silobreaker

15:40 — Networking break

16:10 — Cybersecurity in the age of disorder

Simon Brady, Managing Editor, AKJ Associates Ltd

Pandemic, digitalisation, climate change, the collapse of Chimerica, Brexit – the list goes on. In all this chaos, cybersecurity, like everything else, has to change. But how? In this session, AKJ's Managing Editor, Simon Brady, gives his take on where CISOs should be looking in 2021.

- Stop talking about 'the business' and start understanding it
- From facilities management to strategic advisory, or….?
- Cyber ROI is dead, good riddance to bad rubbish?
- Making use of enforced transparency: a new solution paradigm

16:30 — EXECUTIVE PANEL DISCUSSION — Engaging stakeholders in security: leadership and communication for a cyber-secure business

The transition to remote working and the increasing sophistication of cyber-attacks has forced many organisations to re-evaluate their approach to addressing the human element of risk. Information security professionals need to ensure business stakeholders at all levels are engaged and that their teams are equipped to cope with the changing landscape. Employees are the frontline of cyber-defence: so how can we effectively communicate cybersecurity strategies across the business?

Göran Kördel, CIO, Boliden Group; **Hanne Hansen,** Interim CISO, Ørsted;
Predrag Gaikj, Head of Information Security and Risk Management, Qliro AB; **Andy Dyrcz,** Head of Cyber Security, Linkfire

17:00 — Networking break **17:30** — Conference close

Education Seminars

OneLogin

Empower your employees to work securely and efficiently from home

Stuart Sharp, VP of Solution Engineering, OneLogin

Over the past couple of decades we have seen the number of employees that work from home increase dramatically. Today, due to COVID-19 quarantine policies around the globe, many companies are faced with a new paradigm – employees must work from home for an undefined period of time.

- Adjust to a sudden 100% remote workforce
- Provide easy, secure access to business systems
- Give employees multiple ways to communicate effectively and efficiently
- Ensure device trust and safety flexible authentication policies

Recorded Future

You get what you pay for – pricing on the Nordic underground economy

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

In our digital age, companies that transact business online find their data targeted by various forms of cyber-fraud. These cyber-fraud products and access broker services can be bought and rented freely on the dark web with ease. This is fuelling sophisticated payment systems in the Nordic underground economy.

During this session, we will cover:

- Exclusive access to live threat intelligence feeds from the region
- A detailed review of some of the methods being used in the underground economy
- How to use security intelligence to defend your organisation

Silobreaker

Monitoring threats to areas of operation

Max Mansson, Client Director, Silobreaker

Complementary to traditional cyber-threat intelligence, technical analysis and tactical operations there is a layer of strategic intelligence and context that can often only be gained from the analysis of unstructured web data.

Many organisations have offices, assets or partners around the world, often in locations that have different risk profiles. Using technology to analyse unstructured web data in multiple languages can help maintain visibility into issues that could compromise business processes or security.

This session will cover:

- The ever-changing requirements and responsibilities of threat intelligence teams
- How geopolitical, economic and regulatory trends influence security
- How technology helps monitor the developing threat landscape
- The importance of leveraging unstructured web data

Synack

Can't change the cybersecurity game? Change its structure

Rijk Vonk, Regional Director Benelux & Nordics, Synack

Within companies, cybersecurity has a finite setup; with procedures, protocols, plans and structures all taking up capacity and time. When created, these setups align with available cycles. Today, however, with agile development cycles, we must adjust and align the update cycles with testing cycles. No longer does 'one-size-fit-all' work. And postponing this change is a recipe for disaster.

In this session you will learn:

- How an elite army of global ethical hackers with infinite creativity and tools can help you overcome these challenges
- How these embraced hackers can support you in your fight against hackers with malicious intentions
- And how to let them help you win the infinite game you are up against

Education Seminars

Tripwire

Securing cloud environments, staying on top of cloud configurations to prevent data leaks and inadvertent exposure

Paul Norris, Senior Sales Engineer, Tripwire

As organisations expand further into the cloud, there continues to be an influx of simple mistakes, such as misconfigurations, that can expose organisations to significant security, privacy and regulatory risks. Security teams are stretched, but must stay on top of expanding cloud use and ensure proper security controls are implemented in these environments and maintain compliance over time.

To understand just how well security professionals are implementing industry best practices for cloud security, Tripwire has conducted some detailed research and will share these findings and actionable recommendations for securing the cloud.

The session will cover:

- Current trends on growing cloud usage and security risks involved
- Organisations' biggest concerns when it comes to cloud security
- What steps organisations are taking to secure their cloud environments and where they are having the most challenges
- Recommendations on best practices and technologies available to assist with maintaining security and compliance for the cloud