Post event report

Strategic Sponsors

BeyondTrust

DARKTRACE

ExtraHop

LexisNexis RISK SOLUTIONS

Recorded Future

SentinelOne

VERACODE

Education Seminar Sponsors

CybelAngel

KEYSIGHT TECHNOLOGIES

Menlo Security

RELIAQUEST

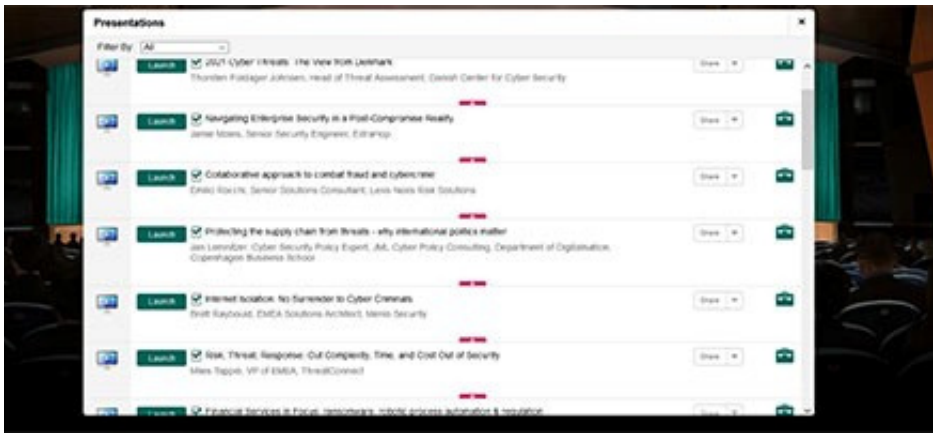
Synack

ThreatConnect

Networking Sponsors

corelight

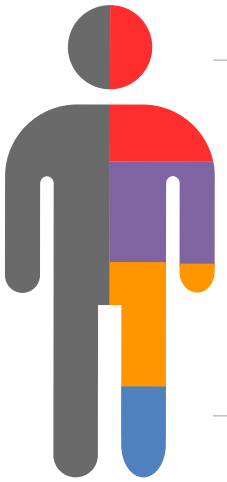
Inside this report:



Key themes

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

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

Emil Bisgaard, Partner, Poul Schmith/Kammeradvokaten

Martin Boreham, Senior Solutions Engineer, BeyondTrust

Simon Brady, Managing Editor, AKJ Associates

Todd Carroll, CISO, CybelAngel

Andy Dyrcz, Head of Cyber Security, Linkfire

Nour Fateen, Presales Manager, UKI & META, Recorded Future

Thorsten Foldager Johnsen, Head of Threat Assessment, Danish Center for Cyber Security

Leena Kuusniemi, Legal Advisor and Founder, Leegal Oy

Thom Langford, Security Advocate, SentinelOne

Jan Lemnitzer, Cyber Security Policy Expert, JML Cyber Policy Consulting, Department of Digitalisation, Copenhagen Business School

Jamie Moles, Senior Security Engineer, ExtraHop

Jörgen Olofsson, Chief Information Security Officer, Praktikertjänst AB

Julia Osseland, Product Marketing Manager, CybelAngel

Joe Partlow, CTO, ReliaQuest

Mariana Pereira, Director of Email Security Products, Darktrace

Brett Raybould, EMEA Solutions Architect, Menlo Security

Emilio Rocchi, Senior Solutions Consultant, Lexis Nexis Risk Solutions

Ashok Sankar, Vice President of Product Marketing, ReliaQuest

Justin Shaw-Gray, Sales Director, Synack Inc.

Dimitrios Stergiou, CISO, Trustly

Miles Tappin, VP of EMEA, ThreatConnect

Julian Totzek-Hallhuber, Solution Architect, Veracode

Mark Walmsley, CISO, Freshfields Bruckhaus Deringer LLP

Andy Young, Security Solutions Architect, Keysight Technologies

Agenda

08:00 Login and networking

08:50 Chairman's welcome

09:00 **2021 Cyber-threats: The view from Denmark**

Thorsten Foldager Johnsen, Head of Threat Assessment, Danish Center for Cyber Security

The latest assessments of the cyber-threats against Denmark, with a focus on cybercrime targeting private companies and what organisations can do.

- Cyberespionage: a threat to your company?
- Cybercrime: the development of organised cooperation between online criminals, new tools, and attack techniques
- Cybersecurity: a decision maker's responsibility

09:20 **Navigating enterprise security in a post-compromise reality**

Jamie Moles, Senior Security Engineer, ExtraHop

- Every organisation gets compromised – it's how fast you detect and respond to an incident that counts
- This is especially important when you look at trends like the overnight move to remote work, the rise in encrypted traffic and acceleration of cloud adoption, as well as the proliferation of enterprise IoT that have expanded the attack surface and complicated the job of security professionals
- We'll explore those trends and the opportunities that lay ahead for security teams post-compromise to prevent an event that results in an outage or an incident from becoming a full-scale data breach

09:40 **Collaborative approach to digital identity and behavioural biometrics to combat fraud and cybercrime**

Emilio Rocchi, Senior Solutions Consultant, Lexis Nexis Risk Solutions

- Risks of the current digitalisation of processes, services and solutions in all industries
- Exponential growth of fraud risks, cybercrimes and financial crimes
- The need for a holistic solution for combatting these threats of fraud and cybercrime whilst protecting the seamless customer experience
- Leverage the intelligence derived from digital identities, behaviour biometrics and behaviour analytics to tackle fraud and cybercrime

10:00 **Protecting the supply chain from cyber-threats – why international politics matters for your company**

Jan Lemnitzer, Cyber Security Policy Expert, JML Cyber Policy Consulting, Department of Digitalisation, Copenhagen Business School

- We have long known how vulnerable we all are to cybercriminals and state hackers, but recent events in international politics have led to revised risk assessments by the national security community. They all point to one conclusion: something needs to be done about cyber-threats, and the protection of critical infrastructure including their supply chains should be a priority
- Regulation is coming: the Biden administration has announced action and the EU is already working on it with its draft NIS 2.0 regulation. The new draft released last December includes a new duty for providers of critical infrastructure to manage cybersecurity risk in their supply chains
- But how can supply chain cyber-risk be managed for hundreds of suppliers when many smaller companies lack a capable IT department? Existing methods involving questionnaires are slow and cumbersome, and require full audits for verification. New startups offering outside-in cybersecurity risk assessments and third-party management tools are rapidly gaining market share, but can they give us the full picture?
- Possible solutions: analysis of current efforts in EU states to set up novel cyber-ratings systems for their national critical infrastructure and the parameters of a future solution to this conundrum

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

Menlo Security

Internet isolation: No surrender to cybercriminals

Brett Raybould, EMEA Solutions Architect, Menlo Security

ThreatConnect

Risk, threat, response: Drive complexity, time, and cost out of your security programme

Miles Tappin, VP of EMEA, ThreatConnect

10:50 Networking break

11:20 **Financial services in focus: Ransomware, robotic process automation and regulation**

Johan Ericsson, Head of Information Security, Entercard Group

- Current drivers for financial fraudsters: investigating rogue actors and protecting your 'low-hanging fruit'
- Ransomware: what are the focused, sophisticated methods organised criminals are now using to get a better ROI for their efforts? How should Information Security Teams respond?
- Embracing robotic process automation and cutting-edge applications. Is it time to switch from DevOps to SecDevOps?
- Regulatory compliance: unique challenges within the financial services, and harnessing the benefits

11:40 **TAKEN: With a vengeance**

Thom Langford, Security Advocate, SentinelOne

"If you leave my network now that will be the end of it. But if you don't, I will look for it, I will find it, and I will pull that kill switch."

In this talk you will learn:

- How to prevent you from having this conversation with cybercriminals
- Why ransomware can exploit even the smallest weakness in your security controls
- Fundamental approaches to detect and respond to minimise and contain damage
- How to take advantage of new services, approaches and attitudes to best curtail any ambitions you have of monologuing like a Hollywood A-lister

12:00 **The value of application security – getting AppSec executive buy in**

Julian Totzek-Hallhuber, Solution Architect, Veracode

- How can you demonstrate the value of adopting or expanding your organisation's Application Security program when there's a growing need for all types of cybersecurity, as well as intense competition for your critical tech budget?
- Join this session to learn how to make the case for AppSec in a way that resonates with executives
- Gain an understanding for which AppSec metrics executives will care about
- Find out how to tie AppSec to corporate goals and priorities

Agenda

12:20 — Changing cyber-landscapes: The battle of algorithms

Mariana Pereira, Director of Email Security Products, Darktrace

- Among rapidly evolving technological advancements, the emergence of AI-enhanced malware is making cyber-attacks exponentially more dangerous and harder to identify. In the near future, we will begin to see supercharged, AI-powered cyber-attacks leveraged at scale
- To protect against offensive AI attacks, organisations are turning to defensive cyber-AI, which can identify and neutralise emerging malicious activity, no matter when, or where, it strikes
- In this session, we will explore the paradigm shifts in the cyber-landscape and the advancements in offensive AI attack techniques and examine real-world examples of emerging threats that were stopped with Cyber-AI

12:40 — Education Seminars | Session 2

Keysight Technologies

How big is your 2021 misconfiguration budget?

Andy Young, Security Solutions Architect, Keysight Technologies

Synack

Next generation defence: Using hackers to beat hackers

Justin Shaw-Gray, Sales Director, Synack Inc., and
Mark Walmsley, CISO, Freshfields Bruckhaus Deringer LLP

13:10 Lunch and networking

14:10 — Fighting fatigue: How an adaptive information security team can keep the business going

Jörgen Olofsson, Chief Information Security Officer, Praktikertjänst AB

- Worker fatigue, especially on the healthcare front-line, has led to an increase in human error. Whilst awareness can help, your information security team should be prepared to accept and mitigate the impact of human error to avoid adding further burden to workers
- At the same time, working from home is here to stay for central office workers. The change in working patterns – extended working hours and the adoption of collaborative tools has impacted network traffic and increased false positives
- User behaviours are no longer clear and predictive. Anomalies are now the norm – what are the best strategies for ensuring your InfoSec teams are aware of the new patterns?
- Is the answer really to initiate new policies, procedures and technology? In this period, initiating change may be destined to fail. An adaptive and considerate approach to information security will enable staff to avoid additional fatigue and keep the business going

14:30 — How to disrupt adversaries with security intelligence

Nour Fateen, Presales Manager, UKI & META, Recorded Future

- How to detect and mitigate cyber-attacks at scale
- How to defend against adversaries constantly improving their techniques and evading defences
- How access to security intelligence empowers organisations to learn about cyber-attacks proactively and take action

14:50 — PAM: Foundational security for business transformation

Martin Boreham, Senior Solutions Engineer, BeyondTrust

- What is digital transformation and why should we care about it?
- Why automation isn't just for the business
- How to mitigate identity risk with Privileged Access Management (PAM)
- How can PAM enable digital transformation

15:10 — Education Seminars | Session 3

CybelAngel

Smart buildings under siege: How IoT brings need to replan your InfoSec strategy

Todd Carroll, CISO, CybelAngel, and
Julia Osseland, Product Marketing Manager, CybelAngel

ReliaQuest

Tackling security in hybrid and multi-cloud environments with confidence

Joe Partlow, CTO, ReliaQuest, and
Ashok Sankar, Vice President of Product Marketing, ReliaQuest

15:40 Networking break

16:00 — Motivating employees to become serious about security: mission impossible?

Leena Kuusniemi, Legal Advisor and Founder, Leegal Oy

- It's all about access management and communication
- How thorough audits can minimise human risk
- BYOD disasters: lessons from the headlines
- The weakest link: how to train your most reluctant employees

16:20 — Delegates will be able to choose from either of the topics below

The skills of the CISO: What does it take to make it in security?

Fireside chat with: Andy Dyrcz, Head of Cyber Security, Linkfire

- CISOs don't have it easy. Achieving the perfect balance of technical know-how, business acumen, risk awareness and regulatory expertise is an uphill battle
- And once there, the role is still often misunderstood or undervalued within the business. This is further proven by the often unrealistic requirements within job adverts in the industry
- Organisations also need to consider how to develop the necessary skills within their security team and put measures in place to nurture the future cyber-workforce
- So, what makes for a superior CISO? And what are the steps for getting there?

Securing third parties and the supply chain

Fireside chat with: Dimitrios Stergiou, CISO, Trustly

- Recent high-profile breaches have reminded organisations of the inherent risks involved in outsourcing services: you are at the mercy of your own vulnerabilities as well as the vulnerabilities of others down the line
- If security vendors are now the target of sophisticated state-actor attacks, and information service providers and government agencies are being hacked by proxy, it begs the question, what hope is there for the rest of us?
- When the security of your third parties is just as integral as your own, what are the approaches organisations need to take to ensure a comprehensive analysis of third-party security risk? And how can we guarantee that brand, reputation, and operations are not open to compromise?

16:40 — Delegates will be able to choose from either of the topics below

How to design contractual requirements regarding cybersecurity

Emil Bisgaard, Partner, Poul Schmith/Kammeradvokaten

- Managing cybersecurity in supplier contracts: areas to include
- Involving relevant stakeholders and senior management in the development of contracts
- Guidance on which cybersecurity themes to consider in supplier contracts and how to implement cybersecurity in supplier contracts

Surviving the cybersecurity revolution

Simon Brady, Managing Editor, AKJ Associates

- Why the return to work is a dangerous moment for security
- Why DX means no more tolerance of failure at the basics
- Left-field lessons from a year of breaches
- What our Nordics research reveals about the region's CISOs

17:00 Closing remarks and networking break

17:30 Conference close

Education Seminars

CybelAngel

Smart buildings under siege: How IoT brings need to replan your InfoSec strategy

Todd Carroll, CISO, CybelAngel, and **Julia Osseland,** Product Marketing Manager, CybelAngel

A blast furnace shut down in a German steel mill... All production lines stopped in an American brewery... Across all industries, connected buildings are becoming prime targets for cyber-attacks. Hackers are quicker than security leaders to recognise blindspots in intertwined IT/OT/IoT environments relying on third-party providers and outsourced systems. By 2023, the financial impact of cyber-physical system attacks as a result of fatal casualties will reach over $50 billion, 10 times higher than 2013 levels of data security breaches. (Source: Gartner, 2020). Good news is, your digital risk protection solution can help you secure your operations against malware and ransomware attacks on smart technologies.

- Understand the risk landscape created by the increasing interconnection of IT, operational technology (OT) and building automation system environments
- Learn how to integrate third-party providers' techs and outsourced systems into your attack surface management strategy
- Discover how CybelAngel can help you bridge the gap between physical security and digital risk protection

Keysight Technologies

How big is your 2021 misconfiguration budget?

Andy Young, Security Solutions Architect, Keysight Technologies

Despite advancements in security, data and security breaches are occurring at an ever increasing rate and severity. Yet, despite the sophisticated range of exploits attackers can employ, they often opt for the path of least resistance. In fact, according to Ponemon, nearly half of all breaches stem from human error, system glitches, and misconfigurations.

Managing a seemingly endless list of patches, updates, and new releases can prove near impossible. Without a way to continuously probe for vulnerable misconfigurations and gaps, it's only a matter of time until hackers find their way in.

Join Andy Young from Keysight Technologies to discover how do you take control of an ever-changing threat landscape and:

- Quantify exposure to specific threat vectors
- Quickly/easily identify & remediate misconfiguration and gaps
- Maximise your existing tools with minimum investment
- Stay ahead of the curve with breach & attack simulation

Menlo Security

Internet isolation: No surrender to cybercriminals

Brett Raybould, EMEA Solutions Architect, Menlo Security

Despite the growing sophistication of cyber-attacks and new pressures of managing remote workers, cyber-practitioners remain defiant in their cyber-defence. No one is ready to wave a white flag. This session is designed for security professionals who are not content to maintain the cyber-status quo and are exploring fundamentally different approaches such as isolation to proactively protect their users and systems.

Join this session to hear two real-world case studies of organisations that have transformed risk of infection at speed and scale – outsmarting threats and promoting productivity.

What will attendees learn:

- How to eliminate risk of infection from browser-based threats
- How to protect users from credential theft via phishing attacks
- How quickly isolation's protective layer around users delivers business value

Education Seminars

ReliaQuest

Tackling security in hybrid and multi-cloud environments with confidence

Joe Partlow, CTO, ReliaQuest, and **Ashok Sankar,** Vice President of Product Marketing, ReliaQuest

With the changing face of business demands, attack surfaces, and technology innovations, cloud computing has firmly entrenched itself as the face of digital transformation in the cybersecurity industry. As organisations mature and devise strategies to adopt and migrate to the cloud, data protection, governance and customer privacy requirements among others are dictating environments that are more than homogenous but hybrid and multi-cloud.

While the cloud has many benefits, there's also hurdles to overcome to increase cloud visibility, detect common cloud attack types and different platforms to understand. Cloud adoption is more of a journey with various stages and it is important that security is baked in considering the various nuances to help detect and prevent misconfigurations and other security threats.

In this session, you'll walk away with:

- An overview of cloud trends and typical attack paths that you need to consider while adopting hybrid and multi-cloud strategies
- Best practices to increase visibility across data that spans multiple cloud platforms (such as AWS, Microsoft Azure, and GCP) to reduce risk
- Examples of how unifying existing on premise and multi-cloud technologies enables faster threat detection and response

Synack

Next generation defence: Using hackers to beat hackers

Justin Shaw-Gray, Sales Director, Synack Inc., and **Mark Walmsley,** CISO, Freshfields Bruckhaus Deringer LLP

There are many dilemmas in today's complex cybersecurity world. Year on year increases in cyber-attacks, an increase in the sophistication of these attacks, a widening cybersecurity talent gap – not to mention IT security budgets that haven't kept up with growing demands.

In this session, Synack's Justin Shaw-Gray will host an open conversation with Mark Walmsley, CISO, Freshfields Bruckhaus Deringer LLP. Justin and Mark will discuss Synack's innovative crowdsourced security model and how Freshfields has ultimately made their platform a more secure place.

Attendees will learn how Freshfields Bruckhaus Deringer LLP:

- Is using an army of ethical hackers to harden corporate assets
- Has transformed and simplified security operations
- Reduced the costs of legacy testing programs
- And is now quickly deploying safer applications

ThreatConnect

Risk, threat, response: Drive complexity, time, and cost out of your security programme

Miles Tappin, VP of EMEA, ThreatConnect

Businesses of all sizes are under constant threat of cyber-attack. Making matters worse, the IoT revolution is enlarging and complicating the cyber-attack surface. Traditional security approaches will no longer work in this new environment, where security teams are drowning in vulnerabilities and alerts.

Join this presentation to learn the game-changing benefits of the new Risk–Threat–Response approach to cybersecurity and risk management.

What attendees will learn:

We will explore each element of the Risk–Threat–Response paradigm in detail.

- *Risk:* Why it is necessary and possible to scope the risk scenarios that matter most to your business from a financial perspective
- *Threat:* Manage the threat landscape with a priority view into the risk scenarios that matter most to your business
- *Response:* Automate & Orchestrate response across the entire security technology stack