Post event report

Strategic Sponsors

BeyondTrust

CROWDSTRIKE

DARKTRACE

Google Cloud

KEYSIGHT TECHNOLOGIES

RANGEFORCE

SentinelOne

Education Seminar Sponsors

cybereason

KENNA Security

onapsis

paloalto NETWORKS

Recorded Future

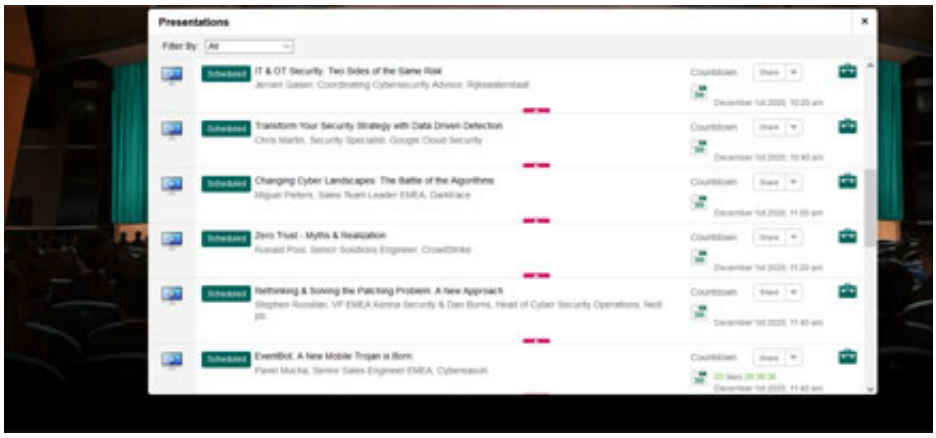
Synack

"As always, e-Crime Benelux remains an excellent event full of insights both from presentations and the resources available. I was apprehensive about the virtual version but the virtual space was beyond anything I have experienced. Navigation was clear and smooth and it was easy to make contact with peers and vendors. Actually, there was additional value to be able to exchange comments during the presentations, on the side-chat. It wasn't too distracting and permitted to clarify questions as they came to mind. All in all, a fantastic experience. Only thing missing were the muffins!"

Data Processing Manager, International Criminal Court

Inside this report:

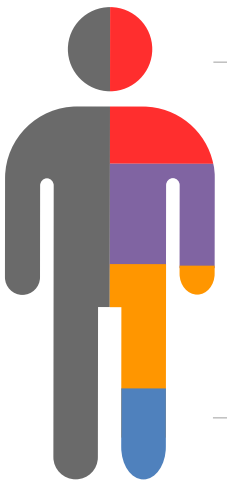
Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars



Key themes

- Cybersecurity for business resilience
- Securing the workplace revolution
- Strengthening identity and access management
- Building in security: easier said than done?
- Securing the customer – are your websites up to it?
- What to do about ransomware?
- Securing digital currencies
- Cybersecurity by remote control
- Securing the citizen
- Stuck in the cloud

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

Martin Boreham, Senior Solutions Engineer, BeyondTrust

Johannes Braams, Senior Cybersecurity Advisor, Royal Haskoning DHV

Simon Brady, Managing Editor, AKJ Associates Ltd

Cosmin Broasca, Business Partner, Security, Risk and BCM, Rabobank

Dan Burns, Head of Cyber Security Operations, Next plc

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

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

Moty Cristal, CEO, NEST

Ronald den Braven, SE Manager Prisma/Access/SaaS EMEA, Palo Alto Networks

Carol Evrard, Intellectual Property, Technology and Data Protection Associate, Wilson Sonsini Goodrich & Rosati

Andrea Foppiani, IT Resilience Manager, Cargill

Jeroen Gaiser, Coordinating Cybersecurity Advisor, Rijkswaterstaat

Daniela Lourenço, Business Information Security Officer, CarNext

Chris Martin, Security Specialist, Google Cloud Security

Gal Messinger, Global Head of Security, Signify

Rene Oskam, Regional VP Benelux & Nordics, Cybereason

Miguel Pieters, Sales Team Leader EMEA, Darktrace

Ronald Pool, Senior Solutions Engineer, CrowdStrike

Stephen Roostan, VP EMEA, Kenna Security

Justin Shaw-Gray, Account Director, Synack Inc.

Eva Telecka, Hub Lead for IT Risk Management and Security, & Liaison Lead EMEA, Merck & Co.

Jan Tietze, Director Security Strategy EMEA, SentinelOne

Mark Walmsley, CISO, Freshfields Bruckhaus Deringer

Frederik Weidemann, Chief Technical Evangelist, Onapsis Inc

Wouter Wissink, Senior Principal Cyber Risk Engineer & PI Tech Europe, Chubb

Andy Young, Security Solutions Architect, Keysight Technologies

Agenda

08:00 Breakfast networking

08:50 Chairman's welcome

09:00 **Engineering for resilience in a complex tunnel system**

Johannes Braams, Senior Cybersecurity Advisor, Royal Haskoning DHV

- What is a complex system?
- How complex is a tunnel system?
- Resilience in the lifecycle of assets
- Various approaches to designing and operating complex systems
- Risk analysis in the light of IEC 62443
- Mitigating measures

09:20 **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 you:

- 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

09:40 **How to secure and manage privileges across every user, session, and asset, every time**

Martin Boreham, Senior Solutions Engineer, BeyondTrust

- Why relying on password management alone leaves dangerous gaps in protection
- Disrupting the cyber-attack chain with privileged access security controls
- Steps to achieving rapid leaps in risk reduction
- Keys to a frictionless PAM solution that is invisible to end users

10:00 **International data transfers: The state of play after Schrems II**

Carol Evrard, Intellectual Property, Technology and Data Protection Associate, Wilson Sonsini Goodrich & Rosati

- International data transfers pre Schrems II
- Schrems II: grounds and decision
- Importance of mapping and evaluating on-going processing (Transfer Impact Assessments)
- Additional measures: what is it?
- Impact on remaining mechanisms: BCRs, SCCs, exemptions
- Need to re-localise your data?
- What is still to be expected: New adequacy decisions, new set of SCCs

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

Palo Alto Networks

Scaling a 'work-from-anywhere' workforce

Ronald den Braven, SE Manager Prisma/Access/SaaS EMEA, Palo Alto Networks

Recorded Future

You get what you pay for – cybercriminal operations in the Benelux underground economy

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

10:50 Break and networking

11:20 **IT & OT security: Two sides of the same risk**

Jeroen Gaiser, Coordinating Cybersecurity Advisor, Rijkswaterstaat

- How IT and OT convergence necessitates a more holistic approach to cybersecurity
- How digitisation imports IT risks like ransomware for OT
- Insights into how Rijkswaterstaat has approached this challenge

11:40 **Transform your security strategy with data driven detection**

Chris Martin, Security Specialist, Google Cloud Security

- Analyse different scenarios and learn how threat actors can use custom-made techniques against your organisation
- Understand how custom detection can provide insight into attacker behaviour
- Adapt to the evolution of the SOC and the changing roles of analysts
- Discover how data-driven detection techniques make your knowledge of your organisation a decisive advantage against attackers

12:00 **Changing cyber-landscapes: The battle of the algorithms**

Miguel Pieters, Sales Team Leader EMEA, Darktrace

- In the face of 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
- Paradigm shifts in the cyber-threat landscape
- Advancements in offensive AI-attack techniques
- How defensive AI can fight back

Agenda

12:20 — Zero trust – myths & realisation

Ronald Pool, Senior Solutions Engineer, CrowdStrike

- The sudden need to facilitate home working this year as a result of COVID-19 meant the corporate network expanded to wherever the user is based. How do we know the users logged into company accounts are who they claim to be when they are working from anywhere?
- A zero trust architecture approach could be the best way to facilitate the most effective security posture for your business right now
- The fundamental concept of zero trust is 'don't trust anybody or anything operating inside or outside your network at any time'. That sounds very pragmatic, but what are the options in this vast playing field full of different definitions?
- Join to hear about: a firm understanding of zero-trust; components of a zero trust architecture; case studies and examples; practical tips

12:40 — Education Seminars | Session 2

Cybereason	Kenna Security
Is XDR the next silver bullet?	**Rethinking & solving the patching problem: A new approach**
Rene Oskam, Regional VP Benelux & Nordics, Cybereason	**Stephen Roostan,** VP EMEA, Kenna Security, and **Dan Burns,** Head of Cyber Security Operations, Next plc

13:10 — Lunch and networking

14:10 — Mistakes management in ransomware negotiations

Moty Cristal, CEO, NEST, and **Gal Messinger,** Global Head of Security, Signify

- Mistakes are an essential element in managing any human crisis, let alone in ransomware and cyber-extortion incidents
- Based on years of operational experience in cyber-crises, and using a variety of real life examples, this session will present the common mistakes made during ransomware crises and how to prevent them
- Hear from first hand experience in successfully negotiating with ransomware criminals

14:30 — Welcome to the future of cybersecurity training!

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

- No more 5 day long, death by PowerPoint, classroom-based courses held in windowless basements in soulless hotels
- No more courses cancelled last minute and no unnecessary travel requirements
- Welcome to on-demand preparation for the real world, using real live VMs simulating real cyber-breach scenarios on a cloud-based platform
- Welcome to selecting your own missions, tailored to you, any time of day or night, learning at your own pace, from the comfort of your own browser

14:50 — How big is your 2021 misconfiguration budget?

Andy Young, Security Solutions Architect, Keysight Technologies

- Maximise your existing tools with minimum investment
- Quickly/easily identify & remediate misconfiguration and gaps
- Step-by-step instructions for fixes and optimal configuration
- Emulate real-world malware and techniques
- Quantify exposure to specific threat vectors
- Stay ahead of the curve

15:10 — Education Seminars | Session 3

Onapsis	Synack
SAP security threat landscape 2021	**Next generation defence: Using hackers to beat hackers**
Frederik Weidemann, Chief Technical Evangelist, Onapsis Inc	**Justin Shaw-Gray,** Account Director, Synack Inc., and **Mark Walmsley,** CISO, Freshfields Bruckhaus Deringer

15:40 — Break and networking

16:00 — Surveying the new cyber-threat landscape: An insurance perspective from the physical world

Wouter Wissink, Senior Principal Cyber Risk Engineer & PI Tech Europe, Chubb

- Anatomy of a cyber-attack
- What we can learn from burglaries and bank robberies in the fight against ransomware
- What will be the next step in ransomware protection?

16:20 — Digital transformation during disruption

Digital transformation was already a driving force prior to the move to mass remote working. Right now, the majority of organisations communicate internally, with customers and with stakeholders through virtual means, have moved to the cloud, and are carried by their apps. For security professionals, attempting to forge a 'safety first' approach during the adoption of new technologies is a headache, even more so when a public health crisis has driven companies into new digital frontiers to keep critical functions running. What happens to your digital transformation journey while chaos rocks the ship?

Cosmin Broasca, Business Partner, Security, Risk and BCM, Rabobank

Andrea Foppiani, IT Resilience Manager, Cargill

Daniela Lourenço, Business Information Security Officer, CarNext

Eva Telecka, Hub Lead for IT Risk Management and Security, & Liaison Lead EMEA, Merck & Co.

16:40 — 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

17:00 — Closing remarks, break and networking

17:30 — Conference close

Education Seminars

Cybereason

Is XDR the next silver bullet?

Rene Oskam, Regional Vice President Benelux and Nordics, Cybereason

We are in a new world where employees need anywhere, anytime access. At the same time the quantity and complexity of the cyber-attacks we face have ramped up. If you're dealing with a single attack on a single asset, today's endpoint detection and response (EDR) tools are all up to task. But can your endpoint technology or SIEM correlate attacks – and more importantly stop those attacks – across all user identities, devices, and endpoints?

Join Rene Oskam for Cybereason in an exploration of this challenge and XDR (extended detection & response) as a potential solution.

You can expect to learn:

- If XDR really is the silver bullet we've been told
- What to keep in mind when looking at XDR solutions
- What the tradeoffs are when implementing XDR
- What comes next after XDR

Kenna Security

Rethinking & solving the patching problem: A new approach

Stephen Roostan, VP EMEA, Kenna Security, and
Dan Burns, Head of Cyber Security Operations, Next plc

In the last six months there has been more pressure than ever on IT security functions to squeeze out as much value as possible from their budgets. In this session, Stephen and Dan look at why the area of vulnerability management offers an untapped opportunity to measurably decrease risk and deliver operational cost savings.

- Strategic and tactical benefits of designing a new framework
- Changing the patching mindset across all stakeholders
- Leveraging existing investments with future-proof, flexible tools
- Defining – and achieving – the right success metrics for your business

Onapsis

SAP security threat landscape 2021

Frederik Weidemann, Chief Technical Evangelist, Onapsis Inc

In the past few years, 64% of organisations' ERP systems have been breached, according to a research study by IDC.

Are you aware how attackers have breached, and can break into unprotected customer SAP landscapes?

Attend this session to gain insights into:

- What attacks on your SAP systems look like
- What security challenges exist in SAP environments (e.g. S/4HANA)
- Moving to the cloud with confidence – how to address security in hybrid landscapes
- Ways to protect your organisation

Palo Alto Networks

Scaling a 'work-from-anywhere' workforce

Ronald den Braven, SE Manager Prisma Access/SaaS EMEA, Palo Alto Networks

Many countries are grappling with implementing and easing lockdowns or restrictions put in place to control the pandemic while organisations continue planning their return to work strategies. As organisations adapt to this new normal, they're widely implementing 'work-from-anywhere' policies for their users and networks. This session shares a perspective on best-practices for enabling a 'work-from-anywhere' workforce in a radically different operating environment, enabling organisations to scale securely.

- What SASE (Secure Access Service Edge) is and the benefits of adopting it
- When you should deploy a cloud-delivered SASE vs. traditional physical or virtual approaches
- How legacy remote access approaches can compromise your organisation
- How the cloud has modernised workforce productivity
- Best practice security capabilities a SASE solution delivers

Education Seminars	
Recorded Future **You get what you pay for – cybercriminal operations in the Benelux 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 on the underground economy in the Benelux. 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
Synack **Next generation defence: Using hackers to beat hackers** **Justin Shaw-Gray,** Account Director, Synack Inc., and **Mark Walmsley,** CISO, Freshfields Bruckhaus Deringer	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.