Post event report

Strategic Sponsors

CROWDSTRIKE

Delinea
Securing identities at every interaction

rubrik

zscaler

Education Seminar Sponsors

Commvault

intruder

Recorded Future

Silverfort

Networking Sponsor

iZOOlogic

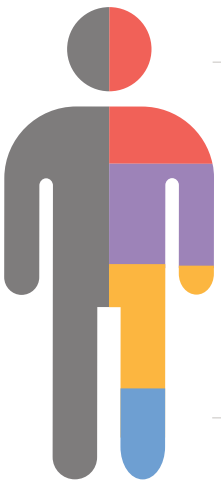
Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

Key themes

- Making the best use of threat intelligence
- Dealing with regulations
- Achieving visibility across ecosystems
- Defending against the latest ransomware variants
- Improving continuous attack surface discovery
- Adversary simulation and behavioural analysis
- Why zero trust, isolation and segmentation are key
- OT and the regulations
- Security posture management
- The power of automation
- Transitioning OT to the Cloud?
- Pen testing for OT / SCADA

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

Dan Andrew,
Head of Security
Intruder

Chris Dearden,
Staff Systems Engineer
Delinea

Martin Dimovski,
Senior DevOps/DevSecOps Engineer
ABN AMRO Bank

Wim Heijs,
Senior Security Engineer
Commvault

Daan Huybregts,
Head of Innovation
Zscaler

Sami Laurila,
GTM Leader Northern Europe Identity & AI Technology
Rubrik

Alan Lucas,
CISO
Worldstream

Gustavo Maniá,
Information Security and Risk Manager (Regional CISO)
HEINEKEN (AME)

Julius Nicklasson,
Sales Engineer
Recorded Future

Vincent Nieuwenburg,
Senior Sales Engineer
CrowdStrike Benelux

Fred Noordam,
Regional Sales Manager Benelux
Silverfort

Ernst Noorman,
Ambassador at Large for Cyber Affairs
Kingdom of the Netherlands

Manit Sahib,
Ethical Hacker, **Cytadel** &
Former Head of Penetration Testing & Red Teaming
Bank of England

Al Scott,
Senior Sales Engineer EMEA
Silverfort

Athina Syrrou,
Senior Director Tech Risk Operations
Booking.com

Elif Yesilbek,
Cryptographer
ABN AMRO

Agenda	
08:20	Breakfast networking & registration
09:20	Chairman's welcome
09:30	**Cybersecurity in geopolitically challenging times** **Ernst Noorman,** Ambassador at Large for Cyber Affairs, Kingdom of the Netherlands • Addressing state-sponsored threats, cyber-warfare, and global tensions • Advancing cyber-diplomacy, regulatory frameworks, and responsible state behaviour • Strengthening multiststakeholder partnerships to enhance cyber-resilience and critical infrastructure security • And what about the resilience of subsea cables?
09:50	**Identity is the new perimeter; combine prevention and recovery to ensure organisational survivability during and after an attack** **Sami Laurila,** GTM Leader Northern Europe Identity & AI Technology, Rubrik • Data & identity focus: How to implement robust cyber-recovery and threat containment across your data and identity estate • Beyond prevention: Ensure rapid response and recovery to minimise downtime and business disruption • Stay operational under attack: How zero-trust architecture helps you maintain control and protect critical data – even during ransomware events
10:10	**FIRESIDE CHAT: Beyond compliance: Building resilient cyber-risk management** **Simon Brady,** Event Chairman (Moderator); **Athina Syrrou,** Senior Director Tech Risk Operations, Booking.com • How can organisations turn risk appetite statements and metrics into practical decision-making tools? • With NIS2 and similar regulations, what does 'appropriate and proportionate' really look like in practice – and how can risk management guide the response? • What makes for strong cyber-risk metrics, and how can CISOs and CSOs give the Board real confidence in the organisation's risk posture? • How does a resilience-first mindset shift culture – from blame and prevention to acceptance, preparedness, and recovery?
10:40	**Education Seminars | Session 1** **Intruder** **Your perimeter is on the front lines: Attack surface reduction as a primary defence** **Dan Andrew,** Head of Security, Intruder **Silverfort** **From reaction to resilience: A new path for privileged access** **Fred Noordam,** Regional Sales Manager Benelux, Silverfort & **Al Scott,** Senior Sales Engineer EMEA, Silverfort
11:20	Networking break
11:50	**Ransomware 3.0: Weaponising AI for the next generation of ransomware attacks** **Manit Sahib,** Ethical Hacker, Cytadel & Former Head of Penetration Testing & Red Teaming, Bank of England • LIVE DEMO – Inside the first AI-powered ransomware attack – See how my custom Agentic Ransomware Gang can take down a network in under 8 minutes • Firsthand insights from real-world red team ops – from legacy tech and broken access controls to the critical lack of real-world security testing • Why traditional security fails – compliance checklists and conventional tools don't stop modern ransomware • What CISOs and security leaders must do now – real-world, field-tested steps to prove your controls work before attackers do it for you

Agenda

12:10 **From control to continuity: Rethinking privileged identity security for the hybrid era**

Chris Dearden, Staff Systems Engineer, Delinea

- Why privileged identities – especially IT admins – are the gateway for today's advanced threats
- What evolving regulations like NIS2 and DORA mean for identity security
- How modern approaches like just-in-time access and privilege elevation reduce standing risk
- Why unified, platform-based PAM strategies are key to sustaining both security and speed

12:30 **Insights from the 2025 Threat Hunting Report**

Vincent Nieuwenburg, Senior Sales Engineer, CrowdStrike Benelux

- The CrowdStrike 2025 Threat Hunting Report reveals how today's most advanced adversaries weaponise AI not only for social engineering but also for reconnaissance, malware enhancement, and vulnerability research, while executing malware-free and cross-domain attacks to bypass defences
- With 81% of hands-on-keyboard attacks malware-free and 320+ organisations infiltrated by AI-enabled insider threats, rapid response is critical
- CrowdStrike's AI-native Falcon platform empowers organisations to detect, disrupt, and stop modern threats

12:50 Lunch & networking break

14:00 **Crypto-agility in the cyber-domain**

Elif Yesilbek, Cryptographer, ABN AMRO

- How cryptography secures digital communications, data, and trust in cyberspace
- The impact of quantum computers on classical cryptography and PQC
- What is crypto-agility and why we need it?

14:20 **Secure connectivity for a critical era: Cellular and the future of infrastructure protection**

Daan Huybregts, Head of Innovation, Zscaler

- As cyber-threats against critical national infrastructure escalate, ensuring secure connectivity is no longer optional – it's essential. This session explores how Zscaler Cellular is transforming the security landscape for critical systems and public sector entities, providing airtight protection against cyber-attacks while enabling seamless operations
- Learn how cellular-native security solutions are redefining resilience for sectors that matter most to public safety and economic stability

14:40 **Education Seminars | Session 2**

Commvault	Recorded Future
From cybersecurity to cyber-resilience	**Hacking the media: The PR tactics of cybercriminals**
Wim Heijs, Senior Security Engineer, Commvault	**Julius Nicklasson,** Sales Engineer, Recorded Future

15:20 Networking break

15:40 **The risks and opportunities that AI brings to cybersecurity**

Gustavo Maniá, Information Security and Risk Manager (Regional CISO), HEINEKEN (AME)

- Real-world AI-driven cyber-risks – from phishing automation to deepfakes and agentic AI threats
- Learn how HEINEKEN manages emerging AI risks while harnessing AI to strengthen defence
- Gain practical insights to help your organisation embrace AI securely and strategically

16:00 **PANEL DISCUSSION** **Securing future architectures**

Simon Brady, Event Chairman, (Moderator);
Martin Dimovski, Senior DevOps/DevSecOps Engineer, ABN AMRO Bank;
Gustavo Mania, Information Security and Risk Manager (Regional CISO), HEINEKEN (AME);
Alan Lucas, CISO, Worldstream;
Manit Sahib, Ethical Hacker, Cytadel & Former Head of Penetration Testing & Red Teaming, Bank of England

- How can security teams design resilient architectures to integrate and leverage emerging technologies such as AI, quantum computing, and IoT?
- What role does AI play in developing proactive rather than reactive security strategies?
- What are the best practices for integrating AI without disrupting legacy systems and existing workflows?
- How can organisations implement zero-trust principles and adaptive access controls to secure ever-evolving environments driven by AI and edge computing?

16:30 Chairman's close

Education Seminars	
Commvault **From cybersecurity to cyber-resilience** **Wim Heijs,** Senior Security Engineer, Commvault	During this session, Wim Heijs from industry leaders Commvault will explore the ideal response for limiting the impact of a cyber-attack and creating a strategic cyber-recovery and resilience plan. Discover how the right strategy can best minimise downtime and ensure business continuity and operational robustness. Cyber-resilience is an ongoing process, so join us to learn how to anticipate, resist and recover from ransomware attacks, quickly restoring your Minimum Viable Company (MVC) and creating the shortest Mean Time to Clean Recovery (MTCR). Attendees will learn: • Not 'If' but 'When'. The importance of refocusing from defensive capabilities in cybersecurity to ensuring a more resilient, optimised approach to response and recovery • How cyber-recovery differs from disaster recovery and what you can do to optimise your organisational posture and cyber-resilience strategy • How to define your Minimum Viable Company (MVC) and the importance of understanding your plan for not just cyber-recovery, but your Mean Time to Clean Recovery (MTCR) post incident
Intruder **Your perimeter is on the front lines: Attack surface reduction as a primary defence** **Dan Andrew,** Head of Security, Intruder	This education seminar will provide a deep-dive into core concepts and practical recommendations for Attack Surface Management (ASM) and asset discovery. Your perimeter is on the front line, and good patch management alone is not enough to protect it. You should leave this session with a better idea of how to blend ASM and asset discovery with patch management for a robust exposure management process. We'll run through examples of attack surface risks, real-world vulnerabilities affecting internet exposed tech, and why implementing an ASM process is critical alongside patch management. It may be tempting to fall back on just patching your biggest 'known' threats, but some of the biggest risks are vulnerabilities that are not yet publicly known. These threats do not have a CVSS score, and attack surface management is your primary defence. Learn how to future-proof your perimeter. Asset discovery is also an essential part of managing your attack surface. Keeping track of your internet exposed IPs and domains is far from trivial, and cloud environments in particular make this challenge harder. Losing track of some of your assets is no longer an embarrassing mistake – it's an unavoidable reality. We will show some examples of how this happens, and give a practical approach to asset discovery which helps you keep track, and avoid systems slipping outside of your exposure management process entirely. Attendees will learn: • Integrating Attack Surface Management into your patch management process – defining ASM as a primary defence that's proactive, not reactive • Prioritisation considerations and why informational risks are criticals waiting to happen. Why not all 'criticals' are equal, and why CVSS is not king • The importance of asset discovery to find shadow IT and build a realistic view of your attack surface. Practical recommendations on how to approach this

Education Seminars	
Recorded Future **Hacking the media: The PR tactics of cybercriminals** **Julius Nicklasson,** Sales Engineer, Recorded Future	This presentation analyses the direct and indirect engagement strategies cybercriminals use to bolster their reputation, increase extortion pressure on victims, and demand more money for stolen data. Defenders can mitigate the impact of these publicity tactics through preparing an intelligence-led incident response plan that includes external communications strategies. Attendees will learn: • How cybercriminals leverage direct and indirect engagement strategies to build their reputation and increase pressure on victims • The specific ways these publicity tactics are used to demand higher ransoms for stolen data • The importance of an intelligence-led incident response plan for mitigating the impact of cybercriminal engagement
Silverfort **From reaction to resilience: A new path for privileged access** **Fred Noordam,** Regional Sales Manager Benelux, Silverfort & **Al Scott,** Senior Sales Engineer EMEA, Silverfort	As identity becomes the new security perimeter, organisations are realising that the most dangerous attacks no longer exploit technical vulnerabilities; they exploit identity. Modern attackers don't break in, they log in. In this session, we explore how enterprises can move from reactive controls to proactive identity resilience. Attendees will learn: • Understand why traditional Privileged Access Management (PAM) methods fall short in today's evolving cyber-threat landscape • Explore a modern, identity-centric approach that builds resilience at the core – moving from reactive controls to proactive defence • Learn about an agentless, continuous strategy for detecting and preventing privileged identity misuse in hybrid and cloud environments • Discover how to reduce attack surfaces, enforce adaptive access policies, and gain granular visibility – without disrupting operational workflows