Post event report

Strategic Sponsors

appurity

cyderes

Lookout

opentext™

RAPID7

rubrik

Saviynt

Inside this report:

Key themes

- Defending against the latest ransomware variants
- OT and the regulations
- Achieving visibility across ecosystems
- Pen testing for OT / SCADA
- Transitioning OT to the Cloud?
- Why zero trust, isolation and segmentation are key

Who attended?

Cyber-security
We have a 20-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

Angus Alderman,
Information Security Officer,
Boden

Christiaan Beek,
Senior Director of Threat Intelligence & Analytics,
Rapid7

Adaora Ezennia,
GRC Lead
THG PLC

Dr Lee Hadlington,
Chartered Psychologist

Matt Johansen,
Vulnerable U podcast Founder,
Advisor & Cyber Security Expert
Rubrik

Muhammad Emal Khan,
Senior Information Security Consultant
Lidl

Klaus Klingner,
Information Security Officer
Asambeauty

Ashish Rajan, CISO,
Enterprise Tech Advisor, Cybersecurity Podcast Host & Speaker
Rubrik

Rory Shannon,
Global VP Engineering
Cyderes

Michael Simpson,
Senior Engineer
Lookout

WaiSau Sit,
Product Marketing Manager
Rubrik

Laurent Strauss,
Cyber Security Strategist
OpenText Cybersecurity

Steve Whiter,
Director of Modern Worker projects
Appurity

Glenn Wilkinson,
Ethical hacker and Ambassador for the Hacking Games

Agenda

08:55 Chairman's welcome

09:00 **The perfect storm – Navigating AI, cyber-resilience and product security across retail supply chains**

Adaora Ezennia, GRC Lead, THG PLC

- The regulatory convergence crisis: CRA, DORA, and EU AI Act are colliding to create overlapping compliance obligations that require integrated strategies, not isolated responses
- The AI supply chain blindspot: Retailers scrutinise vendor cybersecurity but ignore embedded AI systems in supplier operations, creating hidden EU AI Act liabilities and operational risks
- From fragmented audits to unified assurance: A practical framework for third-party monitoring that simultaneously addresses CRA product security, DORA resilience, and EU AI Act transparency
- Action plan: Immediate GRC actions – revise vendor questionnaires, mandate AI disclosures, launch cross-functional risk committees etc

09:20 **Threats in Aisle 7: What Rapid7 labs sees in retail attacks**

Christiaan Beek, Senior Director of Threat Intelligence & Analytics, Rapid7

- The retail industry has become one of the most targeted sectors for modern cybercriminals – from sophisticated social engineering by Scattered Spider to coordinated intrusion campaigns by Crimson Collective
- Rapid7 Labs unveils fresh insights from its global intelligence capabilities, spotlighting how attackers are exploiting retail ecosystems, supply chains, and identity systems for maximum disruption and financial gain
- Learn how Labs' data-driven threat intelligence powers early detection, guides proactive defence, and helps organisations stay one step ahead in the ever-evolving retail threat landscape

09:40 **The AI identity crisis**

Ashish Rajan, CISO, Enterprise Tech Advisor, Cybersecurity Podcast Host & Speaker, Rubrik;
Matt Johansen, Vulnerable U podcast Founder, Advisor & Cyber Security Expert, Rubrik;
WaiSau Sit, Product Marketing Manager, Rubrik

- Explore how AI is reshaping the landscape of identity: from the alarming rise of NHIs to sophisticated social engineering tactics perfected by groups like Scattered Spider
- AI's role in identity attacks: Understand deepfakes, advanced phishing, and the tactics of groups like Scattered Spider
- Proactive identity resilience: Explore a comprehensive approach to securing all facets of identity across your organisation

10:00 **FIRESIDE CHAT: Beyond the store: Securing third-party risk**

Simon Brady, Event Chairman, (Moderator);
Angus Alderman, Information Security Officer, Boden

- How is the evolving threat landscape – ransomware, credential theft, supply chain attacks – shaping your security priorities in retail?
- With so much moving to SaaS, cloud, and outsourced IT, how is the off-prem shift changing your security priorities?
- Retail runs on partners – payments, loyalty apps, delivery, logistics. How do you keep the customer experience smooth without skimping on fraud or identity checks?
- Third parties are often the weakest link. How do you actually monitor them – contracts, frameworks, continuous monitoring, or something else?
- Compliance doesn't stop at your systems. How do you handle PCI, GDPR, and other regulations when data is constantly moving through third parties?
- How are you preparing for the future of retail cybersecurity with AI, IoT, and emerging technologies like quantum-safe cryptography?

10:20 Comfort break

10:25 **Human factors in cybersecurity – Debunking the common myths**

Dr Lee Hadlington, Chartered Psychologist

- Understanding the human role in cybersecurity
- Common myths and misconceptions
- Psychological factors behind security behaviours
- Strategies for building a human-centric cybersecurity culture

10:45 **Modernising identity security for retailers**

Christian Sullivan, Identity and Security Strategist, Saviynt

- Identity is now the #1 attack vector – the new security perimeter for modern retail
- Understand what identity security transformation really means and how to achieve it
- Explore the key challenges facing retailers today: legacy technology, siloed systems, limited resources, and budget pressures
- Learn how to expand the identity security fabric to secure every identity type – human, non-human, third-party, and supply chain
- See how Saviynt helps global retailers modernise identity programs, enhancing security, compliance, and productivity

Agenda

11:05 — Hidden in plain sight: Detecting threats behind the checkout

Laurent Strauss, Cyber Security Strategist, OpenText Cybersecurity

- Retail networks are under constant pressure from credential theft, rogue insiders, and lateral movement through POS and supply chain systems
- We will reveal how AI-driven behavioural analytics can uncover subtle anomalies from data exfiltration to privilege abuse before they escalate into breaches
- Adaptive threat detection, context-aware alerts, and automated investigation workflows enable retailers to reduce dwell time, protect sensitive customer data, and keep operations running smoothly

11:25 — Fortify your future: Mastering business resilience in the digital age

Muhammad Emal Khan, Senior Information Security Consultant, Lidl

- Beyond the firewall: How attacks can shut down operations and new threats can bypass traditional security checks, no longer just about network perimeter defence
- Shared responsibility is non-negotiable: Attendees will learn the critical lesson that 'moving to the cloud' doesn't absolve of responsibility for security
- From paper to practical: You will discover the necessity of moving beyond theoretical planning, lack of practice, results in inadequate preparedness
- The resilience imperative: To strengthen our position, integrating business continuity, crisis management, IT service continuity, and cyber-resilience to ensure operational continuity

11:45 — Comfort break

11:50 — And now the weather forecast – Threat intelligence and SIEMs in the age of cloud computing

Klaus Klingner, Information Security Officer, Asambeauty

- SIEM as radar: Centralise and normalise multi-cloud/SaaS/identity logs; create 'watchlists' for weak signals so small anomalies don't get lost
- Threat intel as forecast: Map sector-specific actor TTPs to MITRE, define watch-conditions (IOCs + behaviours), and pre-stage responses before storms arrive
- ATP as severe-weather alerting: Use automated containment (isolate host, revoke tokens, block IPs) to shrink MTTD/MTTR and close the gap from detection to action
- Cloud = mountain weather: Instrument ephemeral resources (containers, serverless), track config drift, and treat identity and CI/CD as first-class telemetry sources
- Preparedness kit & ritual: Maintain a 3-day 'threat forecast' dashboard, run regular storm-drill tabletops, set clear trigger thresholds, and communicate in plain language to stakeholders

12:10 — Extending the identity fabric

Rory Shannon, Global VP Engineering, Cyderes

- As adversary behaviour changes, we must re-orient detection & response into a more pre-emptive function
- Bringing identity & access management technologies into the threat detection & response process introduces additional friction to the attacker
- Considering the SecOps technology stack holistically allows us to shift SecOps into a prevent first mindset

12:30 — The modern attack chain in retail

Steve Whiter, Director of Modern Worker projects, Appurity;
Michael Simpson, Senior Engineer, Lookout

- Why and how are attackers pivoting to unsecured mobile devices to breach organisations of all types?
- Explanation of mobile focused Tactics, Techniques, and Procedures (TTPs) recently detailed in the NCSC and CISA advisory
- How can you identify any infrastructure gaps that attackers could take advantage of?
- What can be done to remediate the threats exposed to the modern frontline worker?

12:50 — Hacking retail: Real-world attacks and how to stop them

Glenn Wilkinson, Ethical hacker and Ambassador for the Hacking Games

- How attackers target retailers, from ransomware to insider threats
- A live demo of ransomware detonation and its impact on retail systems
- Lessons from high-profile retail breaches (including the M&S Parliamentary Inquiry)
- Practical steps retailers can take to reduce their exposure and respond quickly

13:10 — Chairman's close