Post event report

Strategic Sponsors

Abnormal

BYTES

CLAROTY

CROWDSTRIKE

SENDMARC

SOPHOS

TANIUM

THREATLOCKER®
ZERO TRUST PLATFORM

Inside this report:

Key themes

- Achieving visibility across ecosystems
- Data integrity a critical priority
- Defending against the latest ransomware variants
- Securing Agentic Al
- Why zero trust, isolation and segmentation are key
- From Analysts to Al Supervisors
- Making the best use of threat intelligence
- Security posture management
- Improving continuous attack surface discovery
- The power of automation
- Adversary simulation and behavioural analysis
- Dealing with regulations

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

Callie Baron,
Sr. Content Marketing Manager
AbnormalAI

Tom Butchers,
Cyber Security Strategy & Advisory Lead
Bytes

Harel Ben David,
Director of Market Development
Claroty

Adaora Ezennia,
GRC Lead
THG PLC

Kieran Frost, Chief Operating Officer
Sendmarc

Dan Jones, Senior Security Advisor
Tanium

Boobeshwaran Sengodagoundar Kandasamy, Staff Threat Intelligence Specialist
Deliveroo

Eoin McGrath, Solutions Engineer
ThreatLocker

Rafe Pilling,
Director of Threat Intelligence
Sophos

Richard Plumb,
Threat Operations Lead
Post Office Ltd

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

Mark Ward,
Sr. Regional Sales Engineer
CrowdStrike

Steve Withey,
Principal Security Engineer
ASOS

Agenda	
09:00	Chairman's welcome
09:05	**Threat modelling for operations – The threat-led onboarding model** **Richard Plumb,** Threat Operations Lead, Post Office Ltd • Onboarding systems into the SOC is always a challenge. Knowing what log source to onboard and how to prioritise them isn't always obvious • How do you ensure you're bringing the right log sources onboard without onboarding absolutely everything? • Introducing the threat-led onboarding model. An NCSC tried & tested means to onboarding systems into your SOC • Prioritise log sources, use cases, and making sure every aspect of your SOC is genuinely threat-led
09:25	**This was never a drill: The case for autonomous IT** **Dan Jones,** Senior Security Advisor, Tanium • Why the speed and sophistication of today's retail threat landscape means manual security operations are no longer sufficient – and what that means for how teams must evolve • How autonomous IT works in practice: AI-powered systems that continuously monitor, detect, and remediate threats across endpoints without waiting for human intervention • The real-world business case for autonomous security, including how to identify where automation will have the greatest impact and how to take the first practical steps toward implementation
09:45	**AI-powered threats in retail: Debunking the hype, defining the response** **Tom Butchers,** Cyber Security Strategy & Advisory Lead, Bytes; **Rafe Pilling,** Director of Threat Intelligence, Sophos • Retail organisations are facing an increasingly complex cyber-risk landscape – where AI is accelerating attacks, lowering the barrier to entry for cybercriminals, and reshaping how breaches occur. From identity-driven compromise to ransomware disruption, threats are becoming faster, more targeted, and harder to detect • In this 20-minute fireside chat, Bytes and Sophos will bring a pragmatic, real-world perspective to how adversaries are using AI today – cutting through the hype to explore what's actually happening across the retail sector, and where AI is genuinely transforming the risk landscape • The discussion will also cover how AI is a force multiplier for security teams – accelerating threat discovery, highlighting vulnerabilities and mitigation methods, and empowering teams of agentic SOC analysts, all of which are helping organisations stay ahead of evolving threats • The key takeaway: while attacks are becoming faster and more automated, effective defence is entirely achievable. By focusing on strong cyber-hygiene, identity protection, and integrated, AI-enabled security operations, retail organisations can reduce risk, strengthen resilience, and stay in control
10:05	**Compliance in chaos: The IMS model that puts CISOs back in control** **Adaora Ezennia,** GRC Lead, THG PLC • How to turn overlapping regulations into a coherent, control-driven operating model • How to redesign fragmented RegTech using an Integrated Management System (IMS) that drives clarity, ownership, and efficiency • How to build a defensible compliance posture, with clear accountability and audit-ready evidence, that stands up to regulators, auditors, and legal scrutiny
10:25	Comfort break
10:30	**Scaling security engineering using AI and automation** **Steve Withey,** Principal Security Engineer, ASOS • Risk prioritisation – Understand the current and emerging risks to your business • The AI threat landscape – A high-level coverage of key risks that AI has introduced to businesses • Scaling your teams – Identifying opportunities to innovate and use AI/Automation to scale yourselves • Measure outcomes – What are the key metrics that demonstrate value and success?
10:50	**CrowdStrike 2026 Global Threat Report: A review of key findings** **Mark Ward,** Sr. Regional Sales Engineer, CrowdStrike • Adversaries are becoming more evasive, faster, and harder to stop – leveraging AI and abusing unmanaged edge devices to move rapidly across endpoint, identity, cloud, and SaaS environments, often operating in plain sight • Join us for an in-depth review of the CrowdStrike 2026 Global Threat Report, with a dedicated focus on how these evolving threats are impacting the retail sector • We'll explore real-world implications for retail organisations, share actionable insights, and outline the critical steps needed to strengthen your defences and protect your business in the year ahead

Agenda

11:10	**Two inboxes, one kill chain: Defending retail from the most sophisticated attacks** **Callie Baron,** Sr. Content Marketing Manager, AbnormalAI; **Kieran Frost,** Chief Operating Officer, Sendmarc • In March 2026, Abnormal discovered VENOM, a previously undocumented phishing-as-a-service platform, during its investigation into a credential theft campaign targeting C-suite executives by name across 20+ industries since November 2025 – the campaign neutralises MFA, survives standard remediation, and grants attackers access to trusted executive accounts that can become launchpads for even more damaging attacks • In this 20-minute discussion, Callie Baron (Abnormal AI, co-author of the Exposing VENOM report) and Kieran Frost (COO, Sendmarc) walk the VENOM kill chain and address the concern that matters to retail CISOs: the same impersonation playbook that goes after your execs goes after your customers every day. So what does a defensive posture that covers both actually look like? • This session is built for retail security leaders thinking through the wave that hit M&S, Co-op, Harrods, and the brands that came after		
11:30	Comfort break		
11:35	**Retail threat landscape 2026: What security leaders should prepare for** **Boobeshwaran Sengodagoundar Kandasamy,** Staff Threat Intelligence Specialist, Deliveroo • How retail threats are evolving to become more scalable, automated, and AI-driven – and what that means for your security strategy • Why reactive security approaches are no longer sufficient, and how to adopt a proactive, intelligence-led defence model • Where risks are expanding beyond technology, including brand abuse, social engineering, and supply chain vulnerabilities – and how to address them effectively		
11:55	**Protecting operational technology in modern retail** **Harel Ben David,** Director of Market Development, Claroty • Modern retailers rely on interconnected Operational Technology (OT) throughout the supply chain and in their stores, from AMRs and smart inventory systems to the critical climate controls of the cold chains • Recognise the 'drive-by' threats targeting your critical systems before they disrupt your operations and potentially damage customer trust • Move beyond a tools-only mindset to a resilience strategy that balances people, process, and technology		
12:15	**Make your business a hard target for cybercriminals** **Eoin McGrath,** Solutions Engineer, ThreatLocker • When it comes to potential targets for cyber-attacks, easier to breach means more likely to fall victim • While you might not be able to influence your perceived value, there are changes that can eliminate your organisation from being seen as an easy target • We'll explore practical tactics to reduce your surface area of attack and controls to prevent lateral movement should a breach occur		
12:35	**Invisible leaks: The hidden risks of chatting with AI** **Manit Sahib,** Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England • AI privacy risks: How tools like ChatGPT, Claude, and Co-Pilot can end up knowing more about you than your best friend (and never forget a thing). The hidden dangers of casually sharing information with AI • When small details add up: Why a few 'harmless' details can combine to paint a full picture & how scattered information can reveal sensitive data without you realising • The myth of security: Why AI models aren't as secure as we might think & how attackers can trick them into spilling information • Simple, practical steps: For employees: how to keep personal and company data safe & For organisations: reducing AI-related risks before they grow		
12:55	Chair's closing remarks	**13:00**	End of event