Post event report

e-Crime & cybersecurity CONGRESS

e-Crime & Cybersecurity Congress

11th & 12th March 2026, London

Strategic Sponsors

Abnormal
Akamai
BeyondTrust
CROWDSTRIKE
Delinea
Securing identities at every interaction
HUNTRESS
illumio
intruder
PICUS
proofpoint.
Quorum Cyber
SEARCHLIGHT. CYBER
sublime
THALES
THREATLOCKER®
ZERO TRUST PLATFORM

Education Seminar Sponsors

1Password
Commvault
CONTRAST SECURITY
CYBSAFE
GREYNOISE INTELLIGENCE
HORIZON3.ai
TRUST BUT VERIFY
invicti
LayerX
LMNTRIX
BE THE HUNTER | NOT THE PREY
norm.cyber
OneSpan
RISK LEDGER
rubrik
VARONIS

Networking Sponsors

eSENTIRE
NORD SECURITY
iZOOlogic
ONECOMPLIANCE
ADVISORY | AUDIT | COMPLIANCE
iVerify.

Branding Sponsor

BlackNeuron

Executive Roundtable Sponsor

LayerX

Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

Key themes

Secure everything? Or survive anything?

Preventing a Digital Breakdown

The Accountability Reckoning

From Defence to Design for Failure

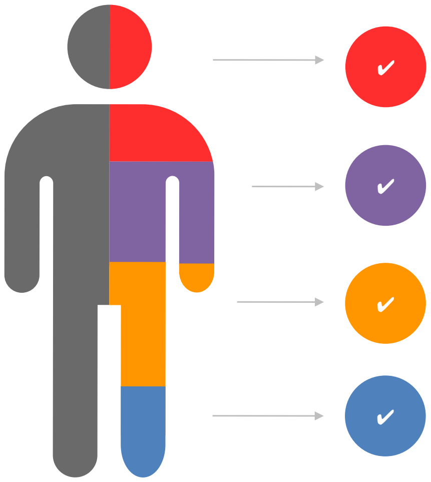
The ROI Reset

Next generation tools and models: the rise of AI

The future of the cybersecurity stack

CISO or Chief Resilience Officer? What's the new power base?

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

Adam Abdat, SOC Lead, **easyJet**; Korhan Acar, Senior Solution Architect, **Picus Security**; Johnson Aduola, Technical Security Officer, **The Royal Marsden NHS Foundation Trust**; Darren Aitchinson, Solutions Architect, EMEA, **Horizon3.AI**; Jack Alexander, Senior Threat Intelligence Consultant, **Quorum Cyber**; Dan Andrew, Head of Security, **Intruder**; Nasser Arif, Cyber Security Manager, **LNWUH NHS Trust**; Dave Barnett, Director Advanced Technology, EMEA, **Proofpoint**; James Beary, Global Sales Director, **CybSafe**; Simon Brady, Event Chairman, **AKJ Associates**; Chris Butchart, Senior Solutions Engineer, **BeyondTrust**; Federico Charosky, Founder & CEO, **Quorum Cyber**; Jarlath Corbett, Solutions Architect, Information Protection, **Proofpoint**; Paul Cragg, Chief Technology Officer, **NormCyber**; Liam D'Amato, Senior Solutions Engineer, **Invicti**; Steve Davies, Head of Cybersecurity, **DLA Piper**; Trevor Dearing, Director, Industry Solutions, **Illumio**; Mike Elliott, Sales Director Northern Europe, **Picus Security**; Robert FitzSimons, Sales Engineer Manager, **Huntress**; John Gilbert, Director Red Lodge Consulting, **OneSpan**; Andy Giles, Executive Director, Cyber & Technology Risk Reporting and Metrics, **JPMorgan Chase**; Mark Grant, Rubrik Cloud & Identity Specialist, **Rubrik**; Holly-Jane Grayling, Security Culture and Awareness Lead, **Tunstall Healthcare**; Romana Hamplova, Pre-Sales Manager for Data Protection, **Thales**; Alex Harris, Head of Gov Cyber Implementation, Government Cyber Unit, **Department for Science, Innovation and Technology**; Paul Hooper, Principal Sales Engineer, **Commvault**; Stephen Kinghan, Senior Manager, Security Risk Specialists, **Lloyds Banking Group**; Justin Kuruvilla, Chief Cyber Security Strategist, **Risk Ledger**; Janette Bonar Law, Information Security Operations Manager, **Channel 4**; Sarah Lawson, Director of Cybersecurity, Risk and Resilience (CISO), **Oxford University Press**; Mick Leach, Field CISO, AbnormalAI; Adam Lorimer, Director of Security Operations, **University College London**; Richard Meeus, Senior Director Security Technology and Strategy, EMEA, **Akamai**; Eoin Molloy, Account Executive, **ThreatLocker**; Céleste Manenc, Corporate Sales Engineer, **CrowdStrike**; Andy Mayle, Senior Manager, Solutions Engineer, **1Password**; Carlo Minassian, Founder & CEO, **LMNTRIX**; Dave Osler, Head of Product, **Searchlight Cyber**; Mike Owen, Deputy Director Cyber Operations, **NHS England**; Zak Pantelli, Distinguished Architect & Senior Director – Data Security & Cryptography, **GSK**; Ian Perry, Head of Sales Engineering, **Searchlight Cyber**; Stephanie Perry, Group CISO, **Babcock International**; Ketan Pyne, Pre-Sales Consultant for Data Protection, **Thales**; Sam Rea, Head of Enterprise Security Architecture, **Bupa Group**; Tom Rossdale, Sales Engineer Director, **Varonis**; Spencer Scott, Global Head of Information Security, **AllSaints & John Varnatos**; David Segev, VP Sales Global Strategic Accounts & International Markets, **Layer X**; Scott Shields, Enterprise Sales Engineer, **Delinea**; Ashish Shrestha (Ash), Former Group CISO, **Jaguar Land Rover**; Dan Strivens, EMEA SE, **GreyNoise Intelligence**; Danielle Sudai, Manager of Security Operations & Automation, **Deliveroo**; Alex Turner, Senior Sales Engineer, **Proofpoint**; Simon Turner, Head of Security Governance and Compliance, **BT Group**; Chris Vaughan, Security Specialist, **Sublime Security**; Chris Wallis, Founder & CEO, **Intruder**; Stuart Wiggins, Horizon Lead, Northern Europe, **CrowdStrike**; Evie Wild, Information Security Officer, EMEA Region, **LBBW Bank**; Seth Williams, Field CTO, **Sublime Securit**y; John Wood, EMEA Sales Director, **Contrast Securit**y; Andrew Yeates, Senior Sales Engineer, **Illumio**; Adeiza Yisa, Business Information Security Office, **Shell**

Agenda | 11th March 2026

08:00 Breakfast & networking break

08:50 Chairman's opening remarks

09:00 **Transforming government cyber: From strategy to delivery**

Alex Harris, Head of Gov Cyber Implementation, Government Cyber Unit, Department for Science, Innovation and Technology

- How government is shifting to a proactive, risk-led cybersecurity model with clear accountability
- What the Government Cyber Action Plan means in practical terms for departments and public sector leaders
- How the new Government Cyber Unit will drive measurable delivery and resilience at scale

09:20 **Never trust, always verify: Why Zero Trust principles remain your best defence against tomorrow's threats**

Chris Butchart, Senior Solutions Engineer, BeyondTrust

- How the 2025 UK retail attacks showed that attackers increasingly 'log in' using stolen or manipulated credentials rather than relying on sophisticated tools
- Why adopting a Zero Trust, identity-centric security model provides a practical roadmap for organisations of any size
- What Non Person Entities (NPEs) are, and why AI agents and automated systems require the same identity and access controls as human users
- Which foundational Zero Trust controls – including PAM, phishing resistant MFA, and deny by default policies – most effectively stop both traditional and AI enabled attacks

09:40 **Proving Zero Trust: AI powered segmentation for real cyber-resilience**

Richard Meeus, Senior Director Security Technology and Strategy, EMEA, Akamai

- Zero Trust is a strategy. Cyber-resilience demands proof. As ransomware, nation/state threats, and AI-driven attacks accelerate, government and enterprise organisations must move beyond static controls and fragmented tools
- This session explores how AI-powered segmentation transforms Zero Trust into a continuously validated risk-containment platform
- Learn how organisations can reduce lateral movement, contain ransomware, secure AI workloads, and prove measurable attack surface reduction across hybrid, cloud, OT, and Kubernetes environments, without disrupting operations
- Walk away with a practical blueprint for turning security architecture into demonstrable resilience

10:00 **Ready to recover: The true test of cyber-resilience**

Andy Giles, Executive Director, Cyber & Technology Risk Reporting and Metrics, JPMorgan Chase

- How the threat has changed – the rise of state-based and hybrid cyber-activity, and the deteriorating threat environment
- Prepare to fail – why resilience incidents are not hypothetical but inevitable, and why readiness must be cultural, not procedural
- Match fit for recovery – what it means to be ready for data and systems restoration under real-world conditions
- Knowing when 'good enough' is good enough – how to measure resilience in ways that are predictive, embedded, and aligned with risk appetite

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

AbnormalAI	**On the front lines of AI-powered email attacks: Stories from a security leader** **Mick Leach,** Field CISO, AbnormalAI
Delinea	**Hackers don't break in anymore, they log in** **Scott Shields,** Enterprise Sales Engineer, Delinea
Intruder	**Your perimeter is on the front lines: Attack surface reduction as a primary defence** **Dan Andrew,** Head of Security, Intruder
OneSpan	**The journey to passwordless: Security, credentials, and lifecycle management** **John Gilbert,** Director Red Lodge Consulting, OneSpan
Picus Security	**Beyond patching: Validating true cyber-exposure** **Korhan Acar,** Senior Solution Architect, Picus Security
Sublime Security	**AI agents Vs GenAI email threats: A practical playbook** **Chris Vaughan,** Security Specialist, Sublime Security
Thales	**Can you keep a secret? Do you control your exposed APIs? And why are they the base of automation?** **Ketan Pyne,** Pre-Sales Consultant for Data Protection, Thales

11:00 Networking break

11:30 **FIRESIDE CHAT: Defending as one – Building national cyber-resilience**

Simon Brady, Event Chairman; Senior NCSC Representative

- Have recent major cyber-incidents changed how NCSC and industry think about cyber-risk – particularly in terms of wider economic and supply chain impact?
- Since most CNI is in the private sector, and a significant proportion of it is foreign owned, what influence does the NCSC actually have?
- How is NCSC's role evolving during major incidents – and what does effective partnership with industry look like in those moments?
- With the Cyber Security & Resilience Bill progressing, what does NCSC most want industry leaders to focus on now to raise the resilience baseline? And what is the ideal balance between detective security and resilience?

11:50 **Why Zero Trust is the answer to securing AI**

Trevor Dearing, Director, Industry Solutions, Illumio

- Who could have guessed that business would still be transforming? This time it is a big one – AI
- How do we protect our AI, protect ourselves from AI, and use AI to protect ourselves?
- Look at how we build resilience into our AI projects and use Zero Trust to save our future

12:10 **CrowdStrike 2026 Global Threat Report: A review of key findings**

Stuart Wiggins, Horizon Lead, Northern Europe, CrowdStrike

- Adversaries are becoming more evasive, faster, and harder to stop – they're leveraging AI and abusing unmanaged edge devices to move rapidly across endpoint, identity, cloud, and SaaS environments while operating in plain sight
- Join us for an in-depth review of the findings from the CrowdStrike 2026 Global Threat Report to gain actionable insights, strengthen your defences, and learn the critical steps needed to protect your organisation in the year ahead

Agenda | 11th March 2026

12:30 **The force multiplier: Navigating the 2026 threat landscape**

Robert FitzSimons, Sales Engineer Manager, Huntress

- The threat landscape continues to change rapidly, and organisations don't always have the team or talent to keep up
- 'Notification Chaos' and 'Human Certainty' seem like distant relatives, but what if you could filter this noise and only receive verified, high-impact threats that actually matter?
- How are hackers leveraging evolving technology and tools to get into our systems, bypass our MFA and compromise our identities
- Understand how everyone can leverage teams with elite threat-hunting techniques, normally only accessible to the Fortune 500

12:50 **Education Seminars | Session 2**

1Password	**Rethinking access, securing the tools and devices you don't control** **Andy Mayle,** Senior Manager, Solutions Engineer, 1Password
Commvault	**Building cyber-resilience for the AI era** **Paul Hooper,** Principal Sales Engineer, Commvault
Contrast Security	**The impact of AI on application risk: From prevention to control** **John Wood,** EMEA Sales Director, Contrast Security
CybSafe	**From awareness training to risk reduction outcomes: The future of human risk management** **James Beary,** Global Sales Director, CybSafe
Layer X	**Shadow AI isn't (just) what you think: How to get visibility into all ai usage in the organisation** **David Segev,** VP Sales Global Strategic Accounts & International Markets, Layer X
Rubrik	**The identity crisis: Building resilience against escalating identity-driven threats** **Mark Grant,** Rubrik Cloud & Identity Specialist, Rubrik
Varonis	**The 2026 attacker's playbook: Hacking trust** **Tom Rossdale,** Sales Engineer Director, Varonis

13:30 Lunch networking break

14:30 **FIRESIDE CHAT: Mitigating cyber-risk across the manufacturing supply chain**

Simon Brady, Event Chairman, (Moderator);
Stephanie Perry, Group CISO, Babcock International

- How can manufacturers gain meaningful visibility into cyber-risk beyond their Tier 1 suppliers without creating excessive complexity or cost?
- As IT and operational systems become increasingly connected, how should organisations manage third-party access and software dependencies within production environments?
- How do you balance robust supply chain security requirements with the need to maintain speed, innovation, and operational continuity?
- When a cyber-incident originates within the supply chain, what distinguishes organisations that recover quickly from those that experience prolonged disruption?

14:55 **Zero Trust controls at the endpoint**

Eoin Molloy, Account Executive, ThreatLocker

- Discover how ThreatLocker applies Zero Trust at the endpoint, eliminating implicit trust by continuously verifying every application, executable, and action before authorisation
- Learn how a deny-by-default, malware-proofing approach reduces ransomware risk, stopping unauthorised software and scripts even when other security layers are bypassed
- Understand how least-privilege enforcement limits attacker capability, ensuring applications and users can perform only explicitly approved actions on enterprise devices
- Explore how granular, policy-based endpoint control safeguards against modern threats, reducing enterprise exposure to ransomware and other advanced attacks

15:00 **AI at breakneck speed: Understanding the risks before it's too late**

Dave Barnett, Director Advanced Technology, EMEA, Proofpoint

- How AI evolved over 70 years, and why Generative AI has achieved the fastest adoption of any enterprise technology
- The security, compliance, and operational risks created by rapid, uncontrolled AI deployment
- Practical steps security leaders can take to enable AI innovation while reducing risk exposure

15:20 **Beyond detection: Why cybersecurity must become preemptive**

Ian Perry, Head of Sales Engineering, Searchlight Cyber

- How external attacker signals provide context to prioritise what truly matters
- Why exploitability – not vulnerability volume – should drive remediation focus
- How exposure management must evolve from visibility and scoring to measurable disruption

15:40 **Post quantum cryptography within life sciences**

Zak Pantelli, Distinguished Architect & Senior Director – Data Security & Cryptography, GSK

- Understanding of PQC and the impact on life sciences
- Why crypto procrastination is causing delay in implementation
- Understanding of PQC migration approaches

16:00 Networking break

16:20 **PANEL DISCUSSION** **Privilege sprawl – the ghost in the machine**

Steve Davies, Head of Cybersecurity, DLA Piper (Moderator); **Adam Lorimer,** Director of Security Operations, University College London; **Adeiza Yisa,** Business Information Security Office, Shell; **Johnson Aduola,** Technical Security Officer, The Royal Marsden NHS Foundation Trust; **Danielle Sudai,** Manager of Security Operations & Automation, Deliveroo; **Sam Rea,** Head of Enterprise Security Architecture, Bupa Group

- How can IAM and Zero Trust expose and contain privilege sprawl before attackers turn it into a breach path?
- What cultural or operational changes are needed to shift from static access models to adaptive, continuously validated security?
- How do we balance usability and functionality in IAM

16:50 Chairman's closing remarks

17:00 Drinks reception

Agenda | 12th March 2026

08:00 Breakfast & networking break

08:50 Chairman's opening remarks

09:00 **When the alarm sounds: The call no leader wants – the human side of being a CISO**

Ashish Shrestha (Ash), Former Group CISO, Jaguar Land Rover

- The psychological and emotional pressure of leading when the organisation is looking to you for answers
- The unseen personal impact as a causality of constant decision cycles and the reality of having no switch-off
- Why organisations plan for operational recovery but rarely prepare leaders for the human toll
- How CISOs can build personal resilience so their leadership remains steady and sustainable under pressure

09:20 **Future-proofing security: Thales' vision for a quantum-safe world**

Romana Hamplova, Pre-Sales Manager for Data Protection, Thales

- Quantum computing will revolutionise industries – but will also expose organisations to unprecedented cyber-risks and new types of cybercrime attacks
- In this session, Thales shares its strategic vision for safeguarding the digital world with post-quantum cryptography
- Discover how Thales is pioneering crypto agility and quantum-safe solutions that empower enterprises to protect critical data, today and tomorrow
- This session will highlight the urgency of quantum resilience aligned with NCSC guidelines, share case studies, and outline the steps global organisations must consider now to future-proof against quantum-enabled threats

09:40 **Privileged identities: The front door of modern cyber-attacks**

Scott Shields, Enterprise Sales Engineer, Delinea

- Why privileged identities are the gateway for today's advanced threats
- Beyond vaulting – learn how to eliminate standing privilege and naturally build cyber-resilience
- How does identity security help evolving regulations like NIS2 and DORA
- Why unified, platform-based PAM strategies are key to sustaining both security and speed

10:00 **FIRESIDE CHAT: Resilience: a revolution or just re-labelling?**

Sarah Lawson, Director of Cybersecurity, Risk and Resilience (CISO), Oxford University Press; **Spencer Scott,** Global Head of Information Security, AllSaints & John Varnatos

- Has 'resilience' actually changed how you run your security operation day to day, or is it mainly a different way of describing the same controls and priorities you already had?
- From 'prevent and protect' to 'ensure continuity of critical services': you still need security, so is this just more work for the security team?
- What investment trade-offs do you now make between prevention and business continuity? Have your technology focuses changed?
- Does a resilience mindset de-prioritise some kinds of breach/loss (e.g. partial customer data, GDPR)? And does it create less of a scapegoating security culture?

10:20 **Education Seminars | Session 3**

GreyNoise Intelligence	**From background noise to actionable intel: Harnessing mass scanning and deception for defence** **Dan Strivens,** EMEA SE, GreyNoise Intelligence
Horizon3.AI	**Beyond compliance: Continuous assurance for real world attack paths** **Darren Aitchinson,** Solutions Architect, EMEA, Horizon3.AI
Invicti	**Shadow AI: AppSec strategies for finding and securing LLM-driven apps** **Liam D'Amato,** Senior Solutions Engineer, Invicti
LMNTRIX	**From hype to advantage: Operationalising AI in the modern SOC** **Carlo Minassian,** Founder & CEO, LMNTRIX
NormCyber	**The quantification of cyber-resilience** **Paul Cragg,** Chief Technology Officer, NormCyber
Quorum Cyber	**Trust is not a control: Identifying Third-party risk with threat intelligence** **Jack Alexander,** Senior Threat Intelligence Consultant, Quorum Cyber
Risk Ledger	**TPRM is broken. Let's fix it together** **Justin Kuruvilla,** Chief Cyber Security Strategist, Risk Ledger

11:00 Networking break

11:30 **Building resilience through experience: Lessons from recent cyber-attacks**

Mike Owen, Deputy Director Cyber Operations, NHS England

- How real-world cyber-attacks unfolded in the NHS, including what worked, what failed, and the practical lessons learned from responding under pressure
- Key strategies for building organisational cyber-resilience, drawn from first-hand experience of managing incidents in a complex, high-impact environment
- Actionable insights leaders can apply immediately to improve preparedness, decision-making, and recovery before, during, and after a cyber-attack

11:50 **Turning the tables: Unlocking your unfair advantage against AI adversaries**

Mike Elliott, Sales Director Northern Europe, Picus Security

- The new reality of 2026: How AI has compressed attack breakout times to just minutes, rendering traditional, reactive defence cycles obsolete
- From static to agentic: Moving beyond manual CTI ingestion to 'Agentic Workflows' that autonomously research, build, and simulate attacks in real-time
- Operationalising autonomy: A deep dive into the four critical AI roles (Researcher, Red Teamer, Simulator, and Coordinator) that bridge the gap between intelligence and remediation
- Pragmatic resilience: Strategies for shifting from 'fixing everything' to focusing on relevant, exploitable gaps, maximising risk reduction while minimising resource drain

12:10 **Malicious vs. Defensive: How AI is changing cybersecurity**

Mick Leach, Field CISO, AbnormalAI

- Are your defences ready for AI-powered email threats? Generative AI now lets attackers launch highly personalised, large-scale phishing and BEC campaigns that slip past traditional red flags and human review
- How will you augment human judgment to keep pace with AI-driven attacks? Pair your people and legacy tools with intelligent, automated detection that learns behavioural patterns and flags subtle anomalies before damage is done
- What steps will you take to put defensive AI in front of malicious AI? Deploy real-time, behaviour-based email security that can detect and stop AI-generated attacks at scale, and turn its insights into concrete actions to harden your defences

Agenda | 12th March 2026

12:30 **Compliance as a consequence: Driving security, enabling assurance – a telco perspective**

Simon Turner, Head of Security Governance and Compliance, BT Group

- Reframing compliance as the natural result of strengthening governance, managing risk, and designing effective controls, rather than treating it as a standalone or periodic activity
- Unifying GRC efforts by embedding clear ownership, aligned controls, and security practices into daily operations while meeting overlapping regulatory and certification requirements
- Strengthening resilience and reducing waste by moving from chasing audit evidence to building systems where compliance is the outcome of doing security the right way

12:50 **Education Seminars | Session 4**

BeyondTrust	**Anatomy of a crisis: Dissecting the 2025 UK retail attacks through a Zero Trust lens** **Chris butchart,** Senior Solutions Engineer, BeyondTrust
CrowdStrike	**AI vs AI: Navigating the new era of the cyber-battlefield** **Céleste Manenc,** Corporate Sales Engineer, CrowdStrike
Huntress	**The kill chain disruptor: Integrating human insights with SOC tradecraft** **Robert FitzSimons,** Sales Engineer Manager, Huntress
Illumio	**Harnessing the OODA loop: Elevating cyber-defence with AI** **Andrew Yeates,** Senior Sales Engineer, Illumio
Proofpoint	**AI is watching… but who's watching your data?** **Jarlath Corbett,** Solutions Architect, Information Protection, and **Alex Turner,** Senior Sales Engineer, Proofpoint
Searchlight Cyber	**Turning the tide on ransomware: Preemptive defence strategies** **Dave Osler,** Head of Product, Searchlight Cyber

13:30 Lunch networking break

14:30 **PANEL DISCUSSION** **Third party and beyond – Where modern breaches begin**

Simon Brady, Event Chairman (Moderator);
Evie Wild, Information Security Officer, EMEA Region, LBBW Bank;
Stephen Kinghan, Senior Manager, Security Risk Specialists, Lloyds Banking Group;
Adam Abdat, SOC Lead, easyJet;
Federico Charosky, Founder & CEO, Quorum Cyber

- How do you identify and manage the potential single point of failure in subcontracting (4th parties)?
- When in-house AI is strictly controlled, how do you manage new AI introduced via third-party add-ons?
- How can you detect and prevent shadow IT and shadow procurement?
- How do you approach changing the culture around the onboarding process?

15:00 **AI, exposure management and the future of pentesting**

Chris Wallis, Founder & CEO, Intruder

- Faced with an overwhelming number of newly discovered vulnerabilities, organisations are turning to CTEM and penetration testing to try and beat the attackers and prevent breaches
- However, each approach comes with very different strengths and weaknesses, meaning organisations have to trade-off cost, frequency, testing time, and depth of checks when choosing how to use them
- The gap between CTEM and penetration testing can seem large, so this talk will explore how AI can act as a bridge between them, and counter-act some of those trade-offs
- We will discuss the role of pentesting as the industry moves towards CTEM, examples of where we've seen AI successfully move the needle, and why even the best agentic systems are not a replacement for the human element

15:20 **Machine vs Machine: Winning the new security arms race**

Seth Williams, Field CTO, Sublime Security

- We stand at the dawn of a new security paradigm where autonomous systems on both sides of the battlefield are changing the dynamics of attack and defence
- Drawing on recent Google Threat Intelligence findings, this session reveals how nation-state actors and cybercriminals are already weaponising AI while showcasing how defensive AI agents can create self-improving security systems
- Learn how the constraints of cost, latency, and efficacy are shaping this machine-vs-machine future, and discover how autonomous agents and domain-specific languages enable a continuous feedback loop to rapidly strengthen defences

15:40 **AI and IT/OT convergence – When models meet motors: AI at the IT/OT edge**

Adeiza Yisa, Business Information Security Office, Shell

- Understand what IT/OT convergence really means in practice and what value AI brings to the mix
- Learn the key architectural and security considerations for integrating AI with legacy IT/OT convergence
- Hear about real-world use cases and measurable outcomes

16:00 Networking break

16:20 **PANEL DISCUSSION** **From human error to human defence – The new era of cyber-culture**

Nasser Arif, Cyber Security Manager, LNWUH NHS Trust (Moderator);
Janette Bonar Law, Information Security Operations Manager, Channel 4;
Holly-Jane Grayling, Security Culture and Awareness Lead, Tunstall Healthcare;
Adeiza Yisa, Business Information Security Office, Shell;
Stephanie Perry, Group CISO, Babcock International

- How can we actively reducing the human and insider attack surface based on the patterns we keep seeing in recent breaches?
- How are you identifying and acting on live behavioural risk signals – beyond training completion – to prevent the next high-impact incident?
- How do we continuously reinforce secure behaviour through in-the-moment nudges, intentional friction, and visibility in daily workflows?
- How are you embedding leadership modelling, accountability, and reinforcement of secure behaviour as a sustained organisational control?

16:50 Chairman's closing remarks

17:00 End of conference

Education Seminars

1Password

Rethinking access, Securing the tools and devices you don't control

Andy Mayle, Senior Manager, Solutions Engineer, 1Password

How do you offboard someone from an app you didn't know they used? Or secure a device you don't manage? In a world of AI agents, shadow IT, and hybrid work, traditional access tools fall short. This session explores how access security must evolve, so you can govern AI, protect unmanaged tools and devices, and empower work without holding teams back.

Attendees will learn:

- Where access security fails in the age of AI agents, shadow IT, and hybrid work
- How to regain visibility and control over apps, tools, and devices you don't own or manage
- Practical approaches to securing access without slowing teams or blocking innovation

AbnormalAI

On the front lines of AI-powered email attacks: Stories from a security leader

Mick Leach, Field CISO, AbnormalAI

Security teams are seeing a rise in highly tailored phishing and business email compromise attacks that look and feel like genuine business communication. In this session, you'll hear a first-hand account from a security leader who believed he had built a best-in-class security stack – until a single email exposed a critical gap.

Through real incidents, including payroll fraud, sextortion, and vendor email compromise, you'll see how attackers exploit trust, urgency, and curiosity to manipulate human behaviour, and why traditional tools and manual review processes fall short. You'll gain a forward-looking view on how AI-driven attacks are evolving and leave with clear steps you can take to reduce human-layer risk, strengthen resilience, and better protect your organisation.

Attendees will learn:

- What can you learn from how AI-powered attacks are hitting peers today? Hear customers walk through real phishing, BEC, and vendor fraud attempts that slipped past legacy tools and looked like everyday business email
- How do you know it's time to change your email security strategy? Learn what inflection points pushed our customers to act, and how they built the business case, aligned executives and the board, and shifted from manual review to AI-driven detection and response
- What would a practical roadmap to defensive AI look like in your organisation? Leave with a clear, customer-tested blueprint – from first steps and quick wins to tuning policies, measuring success, and strengthening resilience while reducing analyst workload

BeyondTrust

BeyondTrust anatomy of a crisis: Dissecting the 2025 UK retail attacks through a Zero Trust lens

Chris Butchart, Senior Solutions Engineer, BeyondTrust

In Spring 2025, Scattered Spider brought several of the UK's largest retailers to their knees in just ten days. One organisation saw hundreds of millions in profit impact; another exposed millions of customer records. Yet the attack chain relied on techniques the industry has known about for years: helpdesk social engineering, SIM swapping, and the abuse of legitimate remote access tools.

This seminar dissects the attacks stage by stage. We'll examine what went wrong, what certain organisations did right to limit damage, and how the same security framework applies just as much to securing AI agents as it does to people.

Attendees will learn:

- How Scattered Spider's attack chain exploited identity weaknesses at every stage, from initial access to ransomware deployment
- Why the NSA mandates Privileged Access Management as a Phase One foundational control – not an advanced capability – in its Zero Trust Implementation Guideline
- The critical differences between organisations that required extended recovery and those that achieved early detection, and what ultimately made the difference

Education Seminars

Commvault

Building cyber-resilience for the AI era

Paul Hooper, Principal Sales Engineer, Commvault

The cyber-attack surface is evolving exponentially. AI-powered threats are exploiting vulnerabilities faster than ever, while cloud-first architectures have created new exposure points demanding fresh protection strategies. The question isn't if your organisation will face an attack – it's when. Will your data be protected? Can your business recover? Join Commvault as we explore the modern threat landscape and demonstrate why an optimised cyber-resilience strategy is imperative.

Attendees will learn:

- How AI is transforming attack velocity and sophistication
- Why cloud-first enterprises must rethink security and recovery
- Practical frameworks for ensuring business continuity when threats become reality
- Real-world lessons from the front lines of enterprise cyber-resilience

Contrast Security

The impact of AI on application risk:
From prevention to control

John Wood, EMEA Sales Director, Contrast Security

AI is accelerating software development beyond the pace traditional security models were designed for. AI-assisted coding increases speed and productivity, but it also changes how vulnerabilities enter applications. Code is generated and modified at scale, often without deep review of every dependency or execution path. The development system has changed – security models built for slower cycles are under strain. Attackers are evolving just as quickly. AI enables faster discovery of weaknesses, quicker adaptation of exploits and lowers the skill required to launch effective attacks. The window between vulnerability introduction and exploitation is shrinking. Relying solely on pre-production controls is no longer realistic.

Vulnerabilities in production are not exceptions – they are inevitable. The strategic question is not how to eliminate every flaw before release, but how to manage risk once software is live. That requires a shift from prevention as the primary control to visibility, containment and response in production. SAST, DAST and secure coding remain essential. But they must be complemented by production-aware controls that distinguish theoretical risk from real, reachable and exploited behaviour. In an AI-accelerated world, resilience depends on understanding what is happening inside running applications – and acting accordingly.

Attendees will learn:

- AI accelerates both delivery and vulnerability discovery
- Pre-production security is necessary but insufficient on its own
- Vulnerabilities in production should be assumed
- Effective risk management requires visibility and control inside live applications

CrowdStrike

AI vs AI: Navigating the new era of the cyber-battlefield

Céleste Manenc, Corporate Sales Engineer, CrowdStrike

Artificial intelligence is changing the pace and scale of cyber-operations. Adversaries are using AI to accelerate reconnaissance, automate intrusion paths, and exploit weaknesses faster than traditional defences can respond. In this session, CrowdStrike shares frontline insight into how this shift is unfolding across the global threat landscape. We examine how threat actors are applying AI today and what effective, AI-native defence looks like in practice. The discussion focuses on practical decision-making, resilience, and how organisations can apply AI with discipline to stay ahead as adversaries continue to evolve.

Attendees will learn:

- How AI is being operationalised by modern adversaries
- Where AI delivers real advantage in detection and response
- What defines an effective AI-native security approach
- How to combine machine intelligence and human expertise to reduce risk

Education Seminars

CybSafe

From awareness training to risk reduction outcomes: The future of human risk management

James Beary, Global Sales Director, CybSafe

The industry is at a turning point in how it understands and manages human cyber-risk. Leading teams are moving beyond awareness training and phishing simulations toward measurable behaviour and real risk outcomes.

Attendees will learn:

- This session explores the forces driving the shift, including the rise of AI, the availability of rich behavioural datasets, the growing importance of scientific evidence and the pressure to automate human risk reduction
- It also challenges a common belief: Many security leaders see themselves as progressive, yet remain anchored in outdated methods that no longer match the threats or the evidence
- This talk provides a roadmap for the future of human-risk management and the steps necessary to lead that change

Delinea

Hackers don't break in anymore, they log in

Scott Shields, Enterprise Sales Engineer, Delinea

The breach didn't start with a zero-day exploit or a sophisticated piece of malware. It started with a username and a password. Today's attackers have figured out that stealing credentials is cheaper, faster, and far more reliable than breaking through technical defences. Identity is the new battlefield but many organisations are fighting the last war. This session cuts through the noise and gives you a practical framework for closing the gaps attackers are actively exploiting right now.

Attendees will learn:

- Why identity is now the #1 attack vector and why traditional perimeter security leaves you exposed
- Practical steps in getting to Zero Standing Privilege and Just-in-Time access, reducing your attack surface without killing productivity
- How attackers move laterally after the initial login and how visibility into privileged sessions stops them in their tracks
- Why machine identities and service accounts are your most exploited blind spot, and what you can do about it today

GreyNoise Intelligence

From background noise to actionable intel: Harnessing mass scanning and deception for defence

Dan Strivens, EMEA SE, GreyNoise Intelligence

This workshop will give participants a fresh perspective and a technical understanding of mass scanning and internet noise, how attackers use those as tools, and how defenders can enhance their perimeter security using data from large scale deception technology, and alongside localised sensor deployments. Given the scale of attacker infrastructure and the speed at which they can deploy exploits against new vulnerabilities, increasing visibility of potential attacks, and distinguishing between what is generic and what is targeted, is of the utmost importance.

Attendees will learn:

- How to use GreyNoise to filter out background noise and hunt for bad actors
- How trends in vulnerability exploitation can help prioritise mitigation and fixes, as well as early warning signals to new vulnerability disclosures
- The place of deception technology in cybersecurity

Education Seminars

Horizon3.AI

Beyond compliance: Continuous assurance for real-world attack paths

Darren Aitchinson, Solutions Architect, EMEA, Horizon3.AI

Compliance frameworks were never designed to stop real attackers – they validate controls at a point in time. Meanwhile, adversaries exploit chains of weaknesses across identity, endpoints, cloud, and third-party access to move laterally and reach critical assets. The result? Organisations that pass audits still suffer breaches.

This session explores how to move beyond compliance toward continuous assurance built around real-world attack paths. Instead of asking, 'Are we compliant?', we ask, 'Can an attacker get from initial access to crown-jewel systems today?' Attendees will learn how dynamic attack path analysis, control validation, and continuous telemetry can expose exploitable paths before they're weaponised – and how to align these insights with risk prioritisation, detection engineering, and executive reporting.

Attendees will learn:

- Why passing audits doesn't equal resilience against multi-stage attacks
- How to identify and prioritise exploitable attack paths across hybrid environments
- How to embed continuous assurance into security operations and risk reporting
- How to translate technical exposure into board-level cyber-risk insight

Huntress

The kill chain disruptor: Integrating human insights with SOC tradecraft

Robert FitzSimons, Sales Engineer Manager, Huntress

Most hackers don't break in – they log in, and they're betting on the fact that you're too buried in 'alert fatigue' to notice them bypassing your MFA in real-time. Learn how to rise above the noise with round the clock peace of mind.

Attendees will learn:

- Learn how SMBs can achieve a 24/7 SOC
- Understand how the Huntress solution can support organisations of any size
- Hear about real-life war stories and how Huntress got involved

Illumio

Harnessing the OODA Loop: Elevating cyber-defence with AI

Andrew Yeates, Senior Sales Engineer, Illumio

Threat actors are more focused than ever on exploiting artificial intelligence to speed up their attacks and improve their effectiveness, fundamentally altering the dynamics of cyber-defence. In this context, the principles of Colonel John Boyd's OODA Loop Observe, Orient, Decide, Act are more relevant than ever, particularly when AI is applied to outpace adversaries operating at machine speed. This discussion explores how Illumio uses AI driven analytics to operationalise the OODA Loop, enabling organisations to detect, understand, and respond to threats faster than human led processes alone can achieve.

Attendees will learn:

- The new risks of pervasive AI in today's world
- Considerations for an effective AI-enabled defence-in-depth strategy
- How to use AI to stay ahead of AI-driven adversaries

Education Seminars

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 will 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

Invicti

Shadow AI: AppSec strategies for finding and securing LLM-driven apps

Liam D'Amato, Senior Solutions Engineer, Invicti

As organisations embed LLMs to accelerate digital innovation, security teams are often left unaware, creating 'shadow AI' risks and new classes of vulnerabilities that traditional testing misses. For most organisations, the challenge isn't building LLMs, it's integrating these token-hungry instances securely. In this session, you will learn how to uncover hidden LLM usage and ensure secure development and testing practices that keep AI-enabled financial applications protected.

Attendees will learn:

- How to identify 'shadow' LLMs and chatbots using advanced fingerprinting and discovery methods
- Enforce AI-integration hygiene through output sanitisation, prompt hardening, access controls, monitoring, and policy alignment
- Detect and prevent attacks that exploit exposed backend LLM tools, plugins, and integrations

Education Seminars

Layer X

Shadow AI isn't (just) what you think: How to get visibility into all AI usage in the organisation

David Segev, VP Sales Global Strategic Accounts & International Markets, Layer X

When we say 'AI,' most people think ChatGPT. And while ChatGPT remains the world's most popular AI tool, AI today comes in a variety of forms, including sanctioned and unsanctioned AI assistants, native SaaS apps with built-in AI chatbots, AI browsers, extensions, desktop applications, and more. This session dives deep into the world of 'shadow' AI and details its various aspects, including unknown apps, hidden identities, unmonitored data channels, and more, and provides a roadmap on how organisations can gain visibility into AI usage in their organisation and how to eliminate shadow AI.

Attendees will learn:

- AI sprawl beyond ChatGPT: The explosion of embedded and native AI across SaaS, browsers, and productivity tools
- The hidden identity problem: Personal accounts, unmanaged tenants, and AI tools operating outside corporate authentication
- Invisible data flows: Sensitive data exposure through AI prompts, uploads, browser-based usage, and shadow integrations
- Why traditional controls fail: CASB, SWG, and DLP limitations in identifying AI activity
- Innovation vs. Governance: How to enable AI adoption while maintaining security oversight
- Gaining real visibility: What 'full AI visibility' actually means – across apps, identities, and sessions
- Executive accountability & risk ownership: How CISOs and security leaders should frame AI risk at the board level

LMNTRIX

From hype to advantage: Operationalising AI in the modern SOC

Carlo Minassian, Founder & CEO, LMNTRIX

AI in cybersecurity is everywhere right now. Copilots, assistants, auto-everything. But here's the thing. Most of it is still surface-level automation dressed up as intelligence. This session cuts through the hype and shows what real, operational AI looks like inside a modern SOC. Carlo Minassian, Founder and CEO of LMNTRIX, shares how an agentic AI approach is being used in production to investigate alerts, reason across telemetry, and execute response actions with humans in the loop. Instead of adding another dashboard or chatbot, LMNTRIX built AI directly into the detection and response workflow.

Attendees will see a live demonstration of Artemis, an autonomous investigation engine that correlates signals across endpoint, identity, cloud, and network, and LISA, a conversational security assistant that explains incidents, recommends actions, and collaborates with analysts in real time via chat and console. The talk walks through what AI is genuinely good at today, where expectations are unrealistic, and how CISOs can apply AI safely and pragmatically to reduce noise, speed investigations, and improve resilience without losing control or transparency. If you care about measurable outcomes like faster investigations, fewer false positives, and less analyst burnout, this session shows what works and what to ignore.

No theory. No slideware. Just real-world AI for cyber-defence, demonstrated live.

Attendees will learn:

- How agentic AI can autonomously triage, investigate, and respond to threats across multiple security layers
- A live walkthrough of Artemis and LISA handling real alerts end to end
- Practical guidance on where GenAI adds value in the SOC and where it doesn't
- How to reduce Tier-1 workload, cut noise, and materially improve MTTD and MTTR without adding more tools

Education Seminars

NormCyber

The quantification of cyber-resilience

Paul Cragg, Chief Technology Officer, NormCyber

2026: The year cyber becomes governable at board level.
Finance has ratios.
Operations have KPIs.
Customer performance has NPS.
Cyber has… dashboards.

Boards are increasingly expected to understand cyber-risk with the same clarity as financial or operational performance. Yet traffic lights, maturity ratings and tool coverage rarely answer a simple business question: How resilient are we to a serious cyber-attack, today? In many organisations that question is hard to answer with confidence. Not because capability is lacking, but because the industry has traditionally optimised for activity and assurance rather than measurable resilience. Meanwhile, risk evolves continuously. Vulnerabilities emerge. Suppliers connect and disconnect. Threat actors adapt. Resilience can drift between periodic assessments while reporting remains static. As regulatory scrutiny intensifies and insurers demand defensible evidence, cyber-resilience must become more than a narrative. It requires management information that is trend-based, explainable, and aligned to recognised frameworks.

This session explores a practical question: What would it mean to treat cyber-resilience as a board-governable metric? Through practical scenarios and open discussion we will examine. This is not about adding more tools. It is about treating cyber as a material business risk that deserves to be measured with rigour. Because what cannot be measured clearly cannot be governed confidently.

Attendees will learn:

- What a defensible, continuously updated resilience construct must include
- Where existing reporting models add value and where they fall short
- How resilience across people, process and technology can be expressed in a way that informs real decision-making

OneSpan

The journey to passwordless: Security, credentials, and lifecycle management

John Gilbert, Director Red Lodge Consulting, OneSpan

As organisations move into 2026, identity continues to sit at the centre of the cyber-threat landscape. Despite years of investment in security controls, passwords remain one of the most consistently exploited weaknesses, underpinning phishing attacks, credential theft, and account compromise across sectors. Passwordless authentication has emerged as a central theme in modern identity and access management strategies. Driven by evolving threat patterns, regulatory pressure, and the limitations of traditional authentication methods, many organisations are now rethinking how users and systems are authenticated, and what 'strong authentication' should look like in practice.

This session will examine how the transition from password to passwordless plays out within real organisational environments. Attention will be given to the practical and operational considerations involved in introducing passwordless approaches, including integration with existing identity systems, organisational readiness, and the impact on both users and administrators. A key area of discussion will be the lifecycle management of authentication credentials. This includes how credentials are provisioned, distributed, recovered, revoked, and replaced over time, and why these processes become increasingly important as organisations adopt phishing resistant authentication methods, including hardware based credentials. The discussion will also consider environments where passwordless adoption can be more complex, such as shared device use, regulated access models, and high staff turnover workforces. Real world considerations will be used throughout to illustrate how organisations can move incrementally toward passwordless without introducing new security or operational risk. Attendees will leave with a clearer understanding of where passwordless fits within a modern identity strategy, and how to approach the journey from passwords to passwordless in a structured and sustainable way.

Attendees will learn:

- Gain practical insight into transitioning from passwords to passwordless
- Understand how to manage credential lifecycles securely and efficiently
- Learn how to address challenges in complex organisational environments
- Discover how to integrate passwordless into your existing identity strategy
- Leave with a structured, low-risk roadmap for sustainable adoption

Education Seminars

Picus Security

Beyond patching: Validating true cyber-exposure

Korhan Acar, Senior Solution Architect, Picus Security

Security teams deal with thousands of critical CVEs, but not all of them are truly exploitable in real environments. This session uses a real-world case study to demonstrate how exposure validation separates theoretical risk from actual attack paths. By continuously testing security control effectiveness and attacker reachability, organisations can focus on the vulnerabilities that genuinely matter and reduce unnecessary remediation efforts.

Attendees will learn:

- Why CVSS and EPSS scores alone are not enough to prioritise risk
- How security control effectiveness changes real-world exploitability
- How to distinguish theoretical vulnerabilities from true attack paths
- How exposure validation provides an attacker's-eye view of risk
- How a real case study helped reduce noise and focus remediation on what truly matters

Proofpoint

AI is watching… but who's watching your data?

Jarlath Corbett, Solutions Architect, Information Protection, Proofpoint &
Alex Turner, Senior Sales Engineer, Proofpoint

As AI and agentic AI are embedded across the enterprise, governing how these systems access and interact with your data becomes critical. Join Proofpoint for a live demonstration exploring three core AI data governance challenges.

Attendees will learn:

- Identifying what AI tools are being used across the business
- Securing and preparing your data for sanctioned AI deployment
- Monitoring AI prompts and interactions to detect data leakage and malicious intent

Quorum Cyber

Trust is not a control: Identifying third-party risk with threat intelligence

Jack Alexander, Senior Threat Intelligence Consultant, Quorum Cyber

Your next breach is unlikely to start inside your organisation. It will start with a supplier.

Attackers choose the easiest route to access, and that route increasingly runs through trusted third parties. Yet many organisations still assess supplier risk through questionnaires and compliance scoring that reveal little about real-world threat activity. Security leaders cannot afford this gap.

This session shows how threat intelligence replaces assumption with evidence. By focusing on real attacker behaviour, external exposure, and active targeting, organisations can identify which suppliers genuinely increase risk and which do not. The result is sharper prioritisation, clearer executive conversations, and more defensible decisions. If you are responsible for managing cyber-risk, this session will reshape how you approach third-party exposure.

Attendees will learn:

- Understand why third parties remain a leading route for compromise
- Identify supplier risk using real threat activity rather than self-reported controls
- Prioritise suppliers based on genuine exposure and attacker interest
- Strengthen board, procurement, and incident response decisions with threat-led insight
- Take practical steps to embed threat intelligence into third-party risk management

Risk Ledger

**TPRM is broken.
Let's fix it together**

Justin Kuruvilla, Chief Cyber Security Strategist, Risk Ledger

Traditional third-party risk management was built for compliance, not real security outcomes. It relies on static questionnaires, fragmented processes and one-to-one supplier views that fail to reflect how modern supply chains actually operate. In this session, we explore why TPRM struggles to reduce risk in practice and how a collaborative, network-driven approach – connecting people, platforms and processes – helps organisations build trust with suppliers, uncover hidden systemic risks, and strengthen resilience across the entire supply chain.

Attendees will learn:

- Why traditional TPRM models struggle to deliver real risk reduction – and where compliance-led approaches fall short in modern, interconnected supply chains
- How a collaborative, network-driven approach helps uncover hidden concentration risk, fourth-party exposure, and systemic weaknesses you can't see in siloed assessments
- Practical ways to move from static questionnaires to continuous, trust-based engagement with suppliers to strengthen resilience across the entire ecosystem

Education Seminars	
Rubrik **The identity crisis: Building resilience against escalating identity-driven threats** **Mark Grant,** Rubrik Cloud & Identity Specialist, Rubrik	Identity-driven threats are exposing a deep structural weakness across modern enterprises. As human and machine identities multiply, they're spilling far beyond the reach of traditional security controls. Organisations are battling credential misuse, lateral movement, misconfigured privileges and fragmented identity stores stretched across cloud, on-premise and SaaS environments. With adversaries now using AI to mine identity data and automate attack chains, many security teams lack the visibility, coordination and operational discipline needed to contain these risks. **Attendees will learn:** • How to compare approaches for modernising identity security • How to embed zero-trust principles • How to build the operational resilience required to support cloud, AI and long-term organisational growth
Searchlight Cyber **Turning the tide on ransomware: Preemptive defence strategies** **Dave Osler,** Head of Product, Searchlight Cyber	Ransomware defence is an achievable goal, though the methods required to maintain it have evolved. As the landscape grows more complex, the most effective strategies move beyond reacting to a breach and focus instead on identifying the activities that precede one. By prioritising visibility into the earlier stages of the attack lifecycle, organisations can address risks before they transition into active incidents. In this workshop, Dave Osler will show how ransomware attacks materialise in their earliest stages and how intelligence-led defence strategies can stop them before they begin. Through demonstrations and real-world case studies, attendees will see how threat actors operate and learn practical techniques to regain the upper hand. By the end of this session, you'll understand how to maintain a continuous view of your attack surface, leverage dark web intelligence to identify threats in their earliest stages, and take decisive action to ensure your organisation isn't an eligible target. **Attendees will learn:** • Early-stage threat detection: From initial access broker posts and forum chatter to exposures in your attack surface • Acting on intelligence: Monitoring dark web activity, investigating warning signs, and taking action before an attack materialises • Preemptive defence strategies: Building continuous monitoring workflows that provide real-time visibility into evolving threats
Sublime Security **AI agents Vs GenAI email threats: A practical playbook** **Chris Vaughan,** Security Specialist, Sublime Security	With recent research showing 1 in 6 data breaches now involve AI-driven attacks, GenAI has accelerated email threats – making them more targeted, scalable, and fast. This new reality outpaces legacy controls, leaving teams waiting on vendor updates. In this session, we'll show a modern approach that pairs an always-updated detection feed with controls adaptive to your organisation, and you'll see our AI agents – the Autonomous Security Analyst (ASA) and Autonomous Detection Engineer (ADE) – working in tandem to clear user-reported queues and propose new detections from real attacks. With clear rationale behind every decision so your team can trust the automation and act immediately, you'll steadily improve coverage without vendor support tickets. You'll leave with a simple rollout checklist and exactly what to measure: catch-rate lift, MTTR/TTM, and noise reduction. **Attendees will learn:** • How GenAI is reshaping email threats: Learn why AI-driven phishing is more targeted, scalable, and fast, and why legacy, one-size-fits-all controls struggle to keep up • How an agentic approach works in practice: Watch how an Autonomous Security Analyst and Autonomous Detection Engineer can triage user-reported emails, investigate real attacks, and generate new detections without vendor tickets • And be left with a practical rollout plan: Get a simple checklist and the key metrics to track, including catch-rate lift, MTTR or TTM improvements, and noise reduction across the abuse mailbox

Education Seminars

Thales

Can you keep a secret? Do you control your exposed APIs? And why are they the base of automation?

Ketan Pyne, Pre-Sales Consultant for Data Protection, Thales

Every infrastructure automation and orchestration is built on APIs and secrets. Your infrastructure exposes thousands of APIs, that require to be continuously detected and protected to avoid data exposure. The access to the APIs is also secured using secrets. Everyone has secrets. You have passwords. Your applications have authentication tokens. Your AI agents use MCP server API keys. The obvious way to keep a secret is to never share it. But software doesn't work that way.

Attendees will learn:

- The art of possible in securing your APIs and secrets, built for the future of automation, aligned with OWASP

Varonis

The 2026 attacker's playbook: Hacking trust

Tom Rossdale, Sales Engineer Director, Varonis

Attackers are no longer just hacking systems. They are hacking trust – exploiting human relationships and digital identities to gain access and move undetected.

In this 2026 planning session, Tom Rossdale will walk you through the entire attack journey, from the first phishing email to the final payload. He'll share real-world examples of the attack techniques we encounter every day, and show you how to stay one step ahead.

Attendees will learn:

- How phishing and social engineering open the door for attackers
- How AI is powering smarter, faster, more personalised attacks
- A detailed walkthrough of the full attack chain
- What's changed since the last attacker's playbook and what to expect going forward