Post event report

Strategic Sponsors

Abnormal
BeyondTrust
CROWDSTRIKE
CultureAI
DeleteMe
FENIX 24
HANDD BUSINESS SOLUTIONS
HOXHUNT
illumio
Pindrop
Ping Identity
proofpoint
SEARCHLIGHT CYBER
SOCRadar Your Eyes Beyond
THREATLOCKER

Education Seminar Sponsors

Commvault
Contrast SECURITY
CYBSAFE
HADRIAN
Silobreaker
Silverfort
TANIUM
VARONIS

Networking Sponsors

CovertSwarm
iZOOlogic
Thomas Murray
DOPE. SECURITY
vicarius
secon.

Branding Sponsors

EASYDMARC
Insight Assurance Delivering Quality, Assuring Trust.
OneSpan

"It is my second year at the e-Crime & Cybersecurity Congress. The sessions are very informative and provide plenty of food for thought! Having many important stakeholders and vendors at the event helps in understanding where the market is going and to have a grasp of the future."

Risk Control Consulting Director, CNA Hardy

"It was very useful to gain perspectives on cybersecurity challenges and how to manage them from a broad spectrum of practitioners in the public and private sectors, and at all levels from individual contributors all the way up to organisational strategic thinkers. The logistical elements of the congress itself were well executed, allowing us as delegates to focus on learning and connecting. I'm happy I attended and would welcome an opportunity to attend again."

Technology Practice Lead, HSBC

"Attending the e-Crime & Cybersecurity event was an incredibly insightful experience. The sessions were highly informative, speakers were top-notch experts. I gained a deeper understanding of current cyber-threats and practical strategies to combat them. Highly recommend!"

President Information Security, Intertek Group

"This conference continues to be the best, and only one, I choose to attend; the presentations enable diverse thinking and opportunity spotting, which is both stimulating and useful to imagining simple solutions to complex problems."

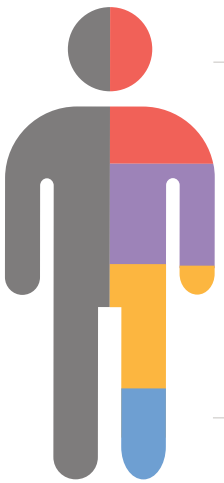
Senior Risk Manager, Close Brothers

Inside this report:

Key themes

- Building a next gen security architecture
- Developing the next generation of security leaders
- Insuring the uninsurable?
- Cybersecurity as a service: the pros and cons
- Cybersecurity for SaaS/IaaS/PaaS
- Making the most of next gen tech: automation, AI and the rest
- Upskilling security teams
- Ransomware – dealing with the new normal
- Embracing digital risk management
- Here come the cybersecurity regulators
- Building better Cloud security
- Can zero trust be done?

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

Michael Adjei, Director, Systems Engineering, Illumio; Noora Ahmed-Moshe, Vice President of Strategy and Operations, Hoxhunt; James Beary, Global Sales Director, CybSafe; Simon Brady, Event Chair, AKJ Associates; William (Bill) J Buchanan OBE, Professor, School of Computing, Edinburgh Napier University; Kushal Dave, Head of Security Operations and Response, Deliveroo; Andy Dreier, Sales Engineer, Varonis; Peter Drissell, Director Aviation Security, UK Civil Aviation Authority; Dan Evans, Head of Cyber Security UK, Vodafone; Robert Fitzsimons, Lead Threat Intelligence Engineer, Searchlight Cyber; Rob Flanders, Head of Threat and Incident Response, BAE Systems Nicole Fowler, CISO, Bank of Ireland; John Gilmore, Director of Research, DeleteMe; Scott Goodall, Commercial Sales Manager UKI, Silverfort; Alex Harris, Head of Future Cyber Capability, Cabinet Office; Craig Hinchliffe, Regional Sales Engineer, CrowdStrike; Phil Huggins, Director for Cyber Policy & NCISO, Health & Care; David Hunt, Senior Product Manager, Silobreaker; Philip Intallura, Group Head of Quantum Technologies, HSBC; Ben Jones, CEO, Searchlight Cyber; Chris Jones, Senior Advanced Consulting Engineer, Tanium; Peter Kaela, Lead Cybersecurity Architect, Scottish Power Energy Networks; Manjesh Kumar, Chief Security Architect/Head of Security Architecture & Risk Services, National AirTraffic Services (Aviation & Aerospace); Alex Laurie, SVP Global Sales Engineering and Go-To-Market Programs, Ping Identity; Ian Littlefair, Head of Cybersecurity, Venator Materials; David Lomax, Senior Engineering Manager, EMEA, Abnormal Security; Heather Lowrie, Independent Advisor & Former CISO of the University of Manchester; James Maude, Field Chief Technology Officer, BeyondTrust; Sumant Mauskar, Senior Vice President, Sales and Global Partners, Pindrop; Alistair Mills, Director, Sales Engineering, Proofpoint; James Moore, CEO, CultureAI; Alexander Myatt, Strategic Account and Partner Relationship Executive, Pindrop; Wendy Ng, BISO, Marks & Spencer; Richard Orange, VP of Sales, EMEA, Abnormal Security; Rob Otto, EMEA Field CTO, Ping Identity; Dave Philpotts, Sales Engineer, Varonis; Jez Reichmann, Deputy CISO, Channel 4; Natalia Shevchuk, SVP, AI Security Architect, Citi; Oliver Simonnet, Lead Cybersecurity Researcher, CultureAI; John Anthony Smith, Founder and Chief Security Officer, Fenix24/Conversant Group; Kev Smith, Strategic Principal Sales Engineer – EMEA, Silverfort; Prash Somaiya, CTO, Hadrian; Valentina Soria, Global Head of Cyber Threat Intelligence, UBS; John Spencer, Engineering Director – Northern Europe, CrowdStrike; Ed Tucker, Cybersecurity CTO, TelefonicaTech Ali Uzun, Senior Solutions Engineer (EMEA & UKI), SOCRadar; Lukas Vaivuckas, Solutions Consultant, Silobreaker; Cdr David Wilcocks MBE, Chief of Staff Cyber Defence At Defence Digital, MoD; Ian Wood, Senior Director EMEA North Sales Engineering, Commvault; John Wood, Senior Regional Sales Manager, Contrast Security; Katie Wood, Information Security Architect, Bibby Financial Services Limited

Agenda | 4th March 2025

08:00 Registration & breakfast networking

08:50 Chairman's welcome

09:00 **When cybersecurity is national security: A challenge in leadership**

Cdr David Wilcocks MBE, Chief of Staff Cyber Defence At Defence Digital, MoD

- How do we motivate and lead our people at the digital frontline?
- Changing our mindset during incident response, at all levels
- Why does it remain a challenge interacting with those outside 'cyber', and how might we demand the leadership that is required?

09:20 **Having an identity crisis in the age of digital dependency**

James Maude, Field Chief Technology Officer, BeyondTrust

- Despite compliance mandates, new technologies and ever increasing budgets, the risk of cyber-attack continues to increase. In this session, James will take a look at the technology, structural and historic challenges that lead organisations to be vulnerable to modern cyber-threats
- Explore how identities are at the heart of breaches and how attackers exploit paths to privilege to win
- Finally look at how modern approaches to identity security and privilege access management can help you fight back

09:40 **Fortify your contact centres against fraudsters**

Sumant Mauskar, Senior Vice President, Sales and Global Partners, Pindrop

- More than 1 in every 730 calls into call centres were fraudulent in 2024
- Deepfake threats are on the rise, becoming more sophisticated and impacting the bottom line (in and out of the call centre)
- Data breaches increased over 78% from the previous year, indicating that bad actors are getting more sophisticated
- Deepfakes pose a fraud risk of $5b to contact centres
- Gain insights in understanding how to navigate and prepare for these complexities and stay ahead in the fight against fraud

10:00 **Business risk management: Building and leveraging threat intelligence to enhance operational resilience**

Valentina Soria, Global Head of Cyber Threat Intelligence, UBS

- Achieving information superiority by transforming vast data into actionable threat intelligence
- Understand how to leverage threat intelligence as a proactive tool for business risk management
- Strategies for integrating intelligence into holistic operational resilience frameworks

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

Commvault	**Cybersecurity to cyber-resilience** **Ian Wood,** Senior Director EMEA North Sales Engineering, Commvault
CrowdStrike	**The ever-evolving threat landscape: Staying ahead of adversaries** **Craig Hinchliffe,** Regional Sales Engineer, CrowdStrike
DeleteMe	**Demystifying challenges in personal data removal** **John Gilmore,** Director of Research, DeleteMe
Hadrian	**How AI can close security gaps before attackers exploit them** **Prash Somaiya,** CTO, Hadrian
Searchlight Cyber	**Gathering intelligence from the dark web** **Robert Fitzsimons,** Lead Threat Intelligence Engineer, Searchlight Cyber
SOCRadar	**Cyber-attacks targeting the UK** **Ali Uzun,** Senior Solutions Engineer (EMEA & UKI), SOCRadar

11:00 Networking break

11:30 **Value of a just culture in cybersecurity – Insights from health and care**

Phil Huggins, Director for Cyber Policy & NCISO, Health & Care

- Understand how to develop a just culture that supports fairness, openness and learning when addressing cyber-vulnerabilities and events
- Supporting organisations to understand and embed a just culture as part of cybersecurity risk management
- Strategies for enabling a positive learning culture that encourages reporting of data security issues

11:50 **Hacking humans for fun and profit**

James Moore, CEO, CultureAI

- How any organisation can be easily breached by targeting almost any employee
- Why humans are the new perimeter
- How the kill chain has evolved to exploit the human perimeter

12:10 **The day-after mindset – A modern cyber-resilience approach**

Michael Adjei, Director, Systems Engineering, Illumio

- The new risks of pervasive AI use in today's world
- How organisations can continue viable business operations after a cyber-incident
- Pragmatic cyber and operational resilience insights for CISOs and security managers
- How to implement complete cybersecurity strategies beyond traditional approaches

12:30 **The trust imperative: Reinventing digital identity for a secure B2B future**

Alex Laurie, SVP Global Sales Engineering and Go-To-Market Programs, Ping Identity

- As digital ecosystems grow more complex, trust is the foundation of secure and seamless B2B interactions
- Learn how AI-driven risk analysis, decentralised identity, and next-gen verification frameworks are redefining digital trust
- Discover strategies to mitigate third-party risks, prevent fraud, and streamline secure access across expanding partner networks
- Explore how organisations can embed trust by design to drive operational efficiency, enhance security, and enable future growth

Agenda | 4th March 2025

12:50	**Education Seminars | Session 2**	
	CultureAI	**Mapping the human perimeter: Understanding and mapping modern cybersecurity threats** **Oliver Simonnet,** Lead Cybersecurity Researcher, CultureAI
	Fenix24/ Conversant Group	**Ransomware in the real world: What no one prepares for** **John Anthony Smith,** Founder and Chief Security Officer, Fenix24/Conversant Group
	Silobreaker	**How to align cyber and geopolitical intelligence to navigate global risks** **Lukas Vaivuckas,** Solutions Consultant, Silobreaker & **David Hunt,** Senior Product Manager, Silobreaker
	Silverfort	**Enhancing privileged access security: Silverfort and Microsoft AD Tiering in action** **Kev Smith,** Strategic Principal Sales Engineer – EMEA, Silverfort & **Scott Goodall,** Commercial Sales Manager UKI, Silverfort
	Tanium	**Harder, Better, Faster, Stronger** **Chris Jones,** Senior Advanced Consulting Engineer, Tanium
	Varonis	**Connecting data security to the identity fabric** **Dave Philpotts,** Sales Engineer, Varonis
13:30	Lunch & networking break	
14:30	Chairman's address	
14:40	**FIRESIDE CHAT: Protecting the connected future**	
	Simon Brady, Event Chair, AKJ Associates, Moderator; **Ed Tucker,** Cybersecurity CTO, Telefonica Tech; **Dan Evans,** Head of Cyber Security UK, Vodafone • With recent incidents like the Salt Typhoon espionage campaign and the Optus breach, how are telcos adapting their security strategies to defend against such sophisticated and large-scale cyber-attacks? • How is the adoption of 5G and edge computing reshaping the network security landscape, and what new challenges does it bring? • With AI increasingly being used for both cyber-attacks and defences, how can telcos harness AI effectively to secure their networks? • What role do partnerships and shared intelligence play in bolstering network security across the telecommunications industry? • How can telcos proactively address regulatory compliance while innovating to secure their critical infrastructure?	
15:00	**The human edge: Evolving security culture in the age of AI**	
	Noora Ahmed-Moshe, Vice President of Strategy and Operations at Hoxhunt • AI is transforming the cybersecurity landscape, enabling attackers to launch highly sophisticated and targeted campaigns • Whilst these threats leverage cutting-edge technology, they remain rooted in timeless psychological tactics – fear, urgency, greed, and curiosity – that exploit human behaviour • Uncover the key skills and leadership strategies essential for fostering a robust cybersecurity culture in the AI era • Learn how to empower your teams to defend against advanced threats by leveraging the human element as a strategic advantage • Receive actionable insights to strengthen your organisation's resilience through a strong cybersecurity culture	
15:20	**Seeing cyber-risk differently: The impact of a human-centric strategy**	
	Alistair Mills, Director, Sales Engineering, Proofpoint • The human-centric defence framework: Discussing how organisations can build stronger defences by focusing on human behaviours, threats, and awareness using real-world examples • Integrated defence: The power of integrating human-centric tools into existing security systems for improved detection, response, and mitigation • Actionable intelligence: Moving beyond traditional defences to deliver real-time, contextual intelligence that addresses human behaviour and risk	
15:40	Networking break	
16:00	**The greatest threat or an amazing opportunity: Quantum computing and cybersecurity**	
	William (Bill) J Buchanan OBE, Professor, School of Computing, Edinburgh Napier University • Understand how quantum computers threaten existing public key encryption methods and their implications on digital security • Learn about NIST's efforts in defining Post Quantum Cryptography (PQC) and how these new methods will protect against quantum threats • Gain insights into the risks of transitioning to PQC and practical strategies for migration • Discover the potential benefits and opportunities quantum computing brings to cybersecurity innovation	
16:30	**EXECUTIVE PANEL DISCUSSION** **Future-proofing security architectures**	
	Simon Brady, Event Chairman & Managing Editor, AKJ Associates (Moderator); **Wendy Ng,** BISO, Marks & Spencer; **Katie Wood,** Information Security Architect, Bibby Financial Services Limited; **Natalia Shevchuk,** SVP, AI Security Architect, Citi; **Manjesh Kumar,** Chief Security Architect/Head of Security Architecture & Risk Services, National Air Traffic Services (Aviation & Aerospace) • How can security teams design resilient architectures to accommodate and leverage new technologies like AI, quantum computing, and IoT? • What role does AI play in developing proactive, rather than reactive, security postures? • Best practices for integrating AI without disrupting legacy systems or existing workflows • How can organisations implement zero-trust principles and adaptive access controls to secure evolving environments driven by AI and edge computing?	
17:00	Drinks reception & networking break	**18:00** End of Drinks reception & networking break

Agenda | 5th March 2025

08:00	Registration & breakfast networking
09:00	Chairman's welcome
09:10	**Building a new approach to government and public sector cybersecurity** **Alex Harris,** Head of Future Cyber Capability, Cabinet Office • An honest review of the current state of government and public sector cybersecurity • Creating a joined-up approach to government and public sector cybersecurity • Meeting the cyber-challenges of the future
09:30	**Key insights for security leaders: CrowdStrike 2025 Global Threat Report** **John Spencer,** Engineering Director – Northern Europe, CrowdStrike • Today's cyber-threat landscape is more complex and interconnected than ever, with adversaries constantly evolving their tactics to exploit vulnerabilities across industries • To combat these threats, organisations must focus on raising the cost of attacks and minimising their impact • The CrowdStrike 2025 Global Threat Report highlights the latest adversary trends, tactics, and events uncovered by CrowdStrike's Counter Adversary Operations team – leaders in threat intelligence and hunting • An in-depth review of the 2025 Global Threat Report findings and gain actionable insights to strengthen your defences and learn the critical steps needed to protect your organisation in the year ahead
09:50	**Why exposed personal data might be your biggest cybersecurity blind spot** **John Gilmore,** Director of Research, DeleteMe • In an era where 353 million users were exposed to identity fraud in 2024 alone, this presentation explores how the 20-year-old issue of personal data privacy has evolved into a critical risk vector for businesses • We'll examine how global trends like remote work and AI-driven technologies have amplified the impact of tactics such as spear phishing and social engineering, making them the most consistently employed methods in successful breaches • Learn why it is worth defending your organisation against these evolving threats by removing employee data from the public web
10:10	**OT cloud architecture, security and resilience by design** **Peter Kaela,** Lead Cybersecurity Architect, Scottish Power Energy Networks • The journey to cloud native, asset-centric security • Platforms and cloud zoning – a defence in depth approach • Unified security strategy, across cloud, OT and CNI considerations
10:30	**Education Seminars | Session 3**
	BeyondTrust — **Paths to privilege – The battleground in identity security** **James Maude,** Field Chief Technology Officer, BeyondTrust
	Contrast Security — **The security gap no one talks about** **John Wood,** Senior Regional Sales Manager, Contrast Security
	Hoxhunt — **Transforming cybersecurity culture: Venator's blueprint for behaviour change building** **Noora Ahmed-Moshe,** Vice President of Strategy and Operations, Hoxhunt & **Ian Littlefair,** Head of Cybersecurity, Venator Materials
	Proofpoint — **Addressing email misdelivery – A human-centric approach** **Alistair Mills,** Director, Sales Engineering, Proofpoint
	Silverfort — **Enhancing privileged access security: Silverfort and Microsoft AD Tiering in action** **Kev Smith,** Strategic Principal Sales Engineer – EMEA, Silverfort & **Scott Goodall,** Commercial Sales Manager UKI, Silverfort
	Varonis — **CISO secrets: Strengthening cyber-resilience in 2025** **Andy Dreier,** Sales Engineer, Varonis
11:10	Networking break
11:40	**Quantum computing and the future of security: HSBC's strategy to combat emerging threats** **Philip Intallura,** Group Head of Quantum Technologies, HSBC • Discover the fundamentals of quantum computing and why HSBC is investing in it for enhanced security and innovation • Examine the potential risks quantum computing poses to existing cryptographic systems • Explore HSBC's initiatives in cryptographic inventory, Post-Quantum Cryptography (PQC), and Quantum Key Distribution (QKD) to ensure quantum safety
12:00	**Security through continuous threat exposure management** **Ben Jones,** CEO, Searchlight Cyber • An overview of the principles of continuous threat exposure management (CTEM) and how they can be practically deployed in organisations • What we mean by continuous: hourly vs daily vs monthly • Real-life examples of identifying, testing, and mitigating vulnerabilities • The role of threat intelligence in continuous threat exposure management

Agenda | 5th March 2025

12:20 — Your backups won't save you

John Anthony Smith, Founder and Chief Security Officer, Fenix24/Conversant Group

- The anatomy of a ransomware breach and how attackers move through environments
- Why backups fail
- What most organisations don't account for in their backup strategies
- Lessons from real-world incidents
- Practical steps to build resilience

12:40 — Education Seminars | Session 4

Abnormal Security	**The AI threat: Protecting your email from AI-generated attacks** **David Lomax,** Senior Engineering Manager, EMEA, Abnormal Security
CybSafe	**Escaping security dogma: How data and evidence are redefining security awareness, culture, and human risk management** **James Beary,** Global Sales Director, CybSafe
Illumio	**Zero trust in an AI world – Moving from talk to action** **Michael Adjei,** Director, Systems Engineering, Illumio
Pindrop	**Fighting misinformation and fraud in a deepfake era** **Alexander Myatt,** Strategic Account and Partner Relationship Executive, Pindrop
Ping Identity	**B2B(2X) under siege: The billion-dollar economy you are funding** **Rob Otto,** EMEA Field CTO, Ping Identity
Tanium	**Harder, Better, Faster, Stronger** **Chris Jones,** Senior Advanced Consulting Engineer, Tanium

13:20 — Lunch & networking break

14:20 — Making UK aviation cyber-safe – A regulator's perspective

Peter Drissell, Director Aviation Security, UK Civil Aviation Authority

- How the CAA has developed cybersecurity oversight of UK aviation
- Achieving effective cybersecurity for UK civil aviation
- How the regulator can become more oil than glue
- What's challenges lie ahead?

14:40 — The importance of AI in threat intelligence and the potential of AI technologies for future threats

Ali Uzun, Senior Solutions Engineer (EMEA & UKI), SOCRadar

- Artificial Intelligence (AI) is revolutionising the field of cybersecurity. As cyber-threats evolve, AI plays a critical role in threat intelligence, enabling organisations to detect, analyse, and respond to attacks more efficiently
- In this webinar, we will explore the key statistics, emerging threats, and future potential of AI in cybersecurity

15:00 — AI in cybersecurity: Defending against the next generation of threats

Richard Orange, VP of Sales, EMEA, Abnormal Security;
Kushal Dave, Head of Security Operations and Response, Deliveroo

- The AI evolution in cybersecurity: How AI is being leveraged by both attackers and defenders
- Combatting AI-powered threats: The growing role of AI in social engineering attacks and how Abnormal Security enhances detection and response
- Business impact & practical benefits: The tangible impact of AI-driven security, from resource allocation to risk reduction
- Future outlook: Predictions on AI's role in cybersecurity over the next 1–2 years and key advice for CISOs navigating AI-driven threats

15:20 — Networking break

15:50 — 0-Day Bingo: Depth in incident response

Rob Flanders, Head of Threat and Incident Response, BAE Systems

- Insights and experiences from BAE Systems on managing cyber-attacks
- Strategies for safeguarding critical infrastructure and supply chain partners
- The growing complexity of the cyber-threat landscape
- Reducing the impact of incidents through proactive defence

16:10 — EXECUTIVE PANEL DISCUSSION — Battling nation-state hackers: Winning the cyber-war

Simon Brady, Event Chairman & Managing Editor, AKJ Associates (Moderator);
Jez Reichmann, Deputy CISO, Channel 4;
Heather Lowrie, Independent Advisor & Former CISO of the University of Manchester;
Robert Flanders, Head of Threat and Incident Response, BAE Systems;
Nicole Fowler, CISO, Bank of Ireland

- How can organisations effectively leverage threat intelligence to proactively counter nation-state attacks? Can they?
- Do regulatory standards actually enhance defence against nation-state actors, or do they merely add compliance burdens without improving security?
- Are we doing enough to address supply chain vulnerabilities, or is this an overlooked entry point for nation-state threats?
- What strategic, forward-looking investments are essential for effectively countering the evolving tactics of APTs?
- Is NCSC guidance genuinely impactful in combating nation-state cyber-attacks?
- In the event of a UK sector-wide cyber-attack are we adequately prepared, and can vendors and service providers effectively handle the pressure of a coordinated response?

16:50 — Chair's closing remarks

17:00 — End of event

Education Seminars	
Abnormal Security **The AI threat: Protecting your email from AI-generated attacks** **David Lomax,** Senior Engineering Manager, EMEA, Abnormal Security	As cybercriminals leverage AI to craft highly sophisticated and targeted attacks, traditional email security solutions are struggling to keep up. In this session, David Lomax, Senior Engineering Manager, EMEA, will explore how AI is reshaping the threat landscape – and how organisations can fight back using AI-driven defences. Attendees will learn: • The evolution of email-based threats and the rise of AI-powered attacks • How cybercriminals use AI to bypass traditional security measures • Why behavioural-based AI is the key to stopping these attacks • Real-world examples of AI-generated threats stopped by Abnormal
BeyondTrust **Paths to privilege – The battleground in identity security** **James Maude,** Field Chief Technology Officer, BeyondTrust	A deeper dive into the world of identity threats, risks and mitigations drawing on examples from real-world attacks. Attendees will learn: • Paths to privilege – the often-overlooked routes that attackers exploit to escalate privileges and access critical systems • The challenges around securing identities and how MFA might not be as secure as you think • Explore common blind spots and misconfigurations that leave organisations vulnerable • This session will include practical recommendations of things to consider for reducing the attack surface in your own environment
Commvault **From cybersecurity to cyber-resilience** **Ian Wood,** Senior Director EMEA North Sales Engineering, Commvault	Threats are exponential, AI is only accelerating, and 'cloud-first' is no longer a distant vision, but the reality of every global enterprise. Join Commvault as they share powerful insights into the constantly evolving cyber-attack surface and demonstrate the importance of why a focus on creating an optimised cyber-resiliency strategy is imperative. Attendees will learn: • Why the traditional model of attack surfaces is not sufficient to describe the evolving threat landscape • The divide between infrastructure and security teams in an organisation and how to bridge it • Why cyber-recovery is more than disaster recovery and how to build an optimal cyber-recovery plan • Building a strategic approach to fully focus on risk, readiness, recovery... and resilience
Contrast Security **The security gap no one talks about** **John Wood,** Senior Regional Sales Manager, Contrast Security	For years, organisations have relied on a simple security model: find vulnerabilities early, fix them before deployment. This approach sounds reasonable – until we confront the reality of modern cyber-threats. Real-world cyber-threats occur against live production applications, not pre-production environments. Cybercriminals exploit gaps – zero-days, unpatched dependencies, and hidden misconfigurations – as soon as they emerge. Join John Wood from Contrast Security to explore the future of application security with real-time protection and intelligence. Attendees will learn: • Why traditional security approaches fail against production threats • How modern attacks bypass static testing and legacy security tools like WAFs • The importance of real-time application security and detection (ADR) • New techniques for measuring risk and building resilient applications

Education Seminars	
CrowdStrike **The ever-evolving threat landscape: Staying ahead of adversaries** **Craig Hinchliffe,** Regional Sales Engineer, CrowdStrike	Cyber-adversaries are evolving rapidly, using sophisticated techniques to breach organisations faster than ever. With breakout times shrinking, security teams have minimal time to detect and respond before damage occurs. To stay ahead, businesses need real-time visibility, proactive intelligence, and AI-powered detection to outpace modern threats. Join CrowdStrike as we dive into the latest intelligence on how adversaries operate and, more importantly, how to stop them before they gain a foothold in your environment. Attendees will learn: • How to identify unknown risks and exposures in real time – Attackers are constantly probing for vulnerabilities, whether in external-facing assets or within cloud environments. Learn how to map and mitigate risks before they become entry points for intrusion • Falcon Shield: What is it? Why is it important? And why now? – Discover how CrowdStrike Falcon Shield is redefining proactive defence, offering real-time attack surface monitoring and automated threat disruption to keep organisations secure against evolving threats • Leveraging AI-powered detection and response to disrupt adversaries faster – With AI-driven detection and intelligence-led response, security teams can move from reactive to proactive defence, neutralising threats before they escalate into full-blown incidents
CultureAI **Mapping the human perimeter: understanding and mapping modern cybersecurity threats** **Oliver Simonnet,** Lead Cybersecurity Researcher, CultureAI	The security game has changed. Your perimeter isn't just your office anymore – it's everywhere your people are. This shift has made understanding human risk critical, transforming our focus from securing individual endpoints to protecting individuals themselves. In this session, we'll explore the concept of the 'human perimeter' and how organisations can develop a structured approach to managing human risk. We'll introduce the concept of human threat mapping to identify and assess the risks posed by employee behaviour in an increasingly decentralised workforce. Attendees will learn: • How the cybersecurity perimeter has evolved over the past decade • Why human risk management is now essential for all organisations and how to integrate this into existing cybersecurity frameworks • The fundamentals of human threat mapping: tools, techniques, and methodologies
CybSafe **Escaping security dogma: How data and evidence are redefining security awareness, culture, and human risk management** **James Beary,** Global Sales Director, CybSafe	Security awareness programmes have long been driven by dogma rather than data, often leading to ineffective and misaligned security outcomes. This session will challenge conventional security thinking and reveal why outdated approaches to security awareness and culture are unravelling. Drawing on behavioural science, data analytics, and real-world evidence, James will highlight key industry shifts, emerging trends, and the critical role of human risk management in modern cybersecurity; demystifying which metrics truly matter, helping security leaders measure and prove the real impact of their efforts. Attendees will learn: • Identifying, targeting, and influencing long-term security behaviours • Quantifying your human cyber-risk • Orchestrating an impactful plan of action with measurable outcomes
DeleteMe **Demystifying challenges in personal data removal** **John Gilmore,** Director of Research, DeleteMe	Scrubbing your digital footprint seems like a simple problem on the surface. But tackling this problem at scale quickly becomes a complex endeavour. Layer on unethical vendor practices and misleading claims of effectiveness and the picture suddenly becomes murky and confusing to navigate. Attendees will learn: • What you need to understand about data removal claims and ethical practices • How vendors are reporting on efforts and obfuscating actual results

Education Seminars	
Fenix24/Conversant Group **Ransomware in the real world: What no one prepares for** **John Anthony Smith,** Founder and Chief Security Officer, Fenix24/Conversant Group	Most organisations believe their cybersecurity programme includes a clear path to recovery after a ransomware attack. In reality, it's the hidden complications that cause businesses to suffer the most. This session breaks down the breach patterns that lead to widespread failures, the tactics of modern-day threat actors, and the critical missteps most organisations make when securing their backups. Attendees will learn: • How ransomware attacks unfold • Why 'having backups' isn't the same as being able to recover • Why restoration isn't just about data, but full business operations • Proven recovery strategies that minimise downtime and financial loss
Hadrian **How AI can close security gaps before attackers exploit them** **Prash Somaiya,** CTO, Hadrian	As attack surfaces expand, the ability to maintain clear visibility over assets, vulnerabilities, and threats is becoming increasingly difficult. Threat actors are automating reconnaissance, weaponising exploits faster than ever, and identifying blind spots before security teams do. If organisations continue to rely on slow, reactive security, they will always be one step behind. The key to staying ahead? Radical visibility and continuous, real-time security validation. Attendees will learn: • Attackers have automated the discovery of assets and weak points • AI is shortening the exploit cycle from months to minutes • Proactively secure your environment with real-time offensive insights
Hoxhunt **Transforming cybersecurity culture: Venator's blueprint for behaviour change building** **Noora Ahmed-Moshe,** Vice President of Strategy and Operations, Hoxhunt & **Ian Littlefair,** Head of Cybersecurity, Venator Materials	Building a strong security culture is critical for addressing the human element in cybersecurity. In this session, Noora Ahmed Moshe, Vice President of Strategy and Operations at Hoxhunt, and Ian Littlefair, Head of Cybersecurity at Venator Materials – a global leader in the chemical industry – share how Venator successfully transformed its cybersecurity strategy by embedding behaviour change into its culture. Gain insights into how Venator tackled human risk management challenges, implemented tailored training programmes, and fostered psychological safety to empower its workforce. Learn how leadership alignment, positive reinforcement, and actionable insights can drive meaningful behaviour change and resilience against evolving threats. Attendees will learn: • How Venator overcame key challenges in managing human risk • The role of tailored, continuous training in fostering secure behaviours • Strategies to create a culture of psychological safety that encourages positive engagement • Why leadership alignment and data-driven insights are essential for sustained change • Proven techniques to transform employees into your strongest cybersecurity defence
Illumio **Zero Trust in an AI world – Moving from talk to action** **Michael Adjei,** Director, Systems Engineering, Illumio	In the face of evolving threat landscape, it is no longer a matter of if you are targeted by threat actors but rather when you are targeted. This fact is further amplified by the pervasive use of AI across various digital platforms today. How can organisations set themselves up to survive and thrive after an attack? This session will focus on how to implement zero trust principles to ensure critical business operations can continue during and after a cyber-incident. Attendees will learn: • Rethinking cyber-resilience in favour of ease of operationalisation • Key considerations for an effective defence-in-depth strategy • Pragmatic steps on business continuity through an adaptive security posture

Education Seminars	
Pindrop **Fighting misinformation and fraud in a deepfake era** **Alexander Myatt,** Strategic Account and Partner Relationship Executive, Pindrop	AI-powered voice fraud is a major cybersecurity threat. Pindrop will show how criminals use synthetic voices to bypass authentication, demonstrate real attacks, and present solutions to detect and combat this threat. It's time to rethink voice security in the AI era. Attendees will learn: • AI is changing the way we see and hear information. With the rise of deepfakes, so does misinformation and fraud • The human ear can detect synthetic voice only 60% of the time. How do we close the 40% gap? • Learn how deepfakes are becoming more sophisticated and how 'good AI' needs to be ready to combat 'bad AI'.
Ping Identity **B2B(2X) under siege: The billion-dollar economy you are funding** **Rob Otto,** EMEA Field CTO, Ping Identity	In the era of B2B(2X), where organisations must seamlessly connect with customers, partners, and suppliers, identity must be treated as the new security perimeter. Traditional authentication methods are failing, leaving businesses exposed to costly breaches, operational disruption, and reputational damage. Security leaders must rethink identity strategies to stay ahead. This session will break down the latest innovations in identity security – so you can eliminate threats before they strike, enable frictionless user experiences, and future-proof your organisation against the competition. If you think MFA is enough, think again. Identity is your first line of defence, how will you ensure it's built to win? Attendees will learn: • B2B(2X) at risk – How stolen credentials and third-party access create new vulnerabilities in extended business ecosystems • AI-powered fraud is here – How attackers are using automation to bypass traditional identity defences • Beyond passwords: The future of authentication – passkeys, behavioural biometrics, and invisible security • Frictionless, secure access – Achieving airtight security while ensuring seamless B2B(2X) interactions • Lessons from the front lines – How leading enterprises are securing identity across B2B(2X) networks
Proofpoint **Addressing email misdelivery – A human-centric approach** **Alistair Mills,** Director, Sales Engineering, Proofpoint	Email misdelivery is a persistent yet often overlooked risk in cybersecurity. Whether it's sending sensitive information to the wrong recipient or accidental exposure of confidential data, the consequences of email misdelivery can be severe. Attendees will learn: • The risk of email misdelivery: Understanding the types of misdelivery events and their potential impact on data security, compliance, and business reputation • AI-powered prevention: How machine learning and behavioural analytics can automatically detect and prevent email misdelivery before it happens • Integrating email security: The benefits of combining email misdelivery protection with broader human-centric security strategy for comprehensive risk mitigation
Searchlight Cyber **Gathering intelligence from the dark web** **Robert Fitzsimons,** Lead Threat Intelligence Engineer, Searchlight Cyber	In this seminar, Searchlight Cyber will walk through real-life case studies to demonstrate how organisations can effectively gather intelligence from the dark web to inform their security, based on extensive work with both public and private sector entities. Attendees will learn: • How to identify an active threat against your organisation by monitoring dark web sites • Spotting exploit development to inform CVE prioritisation and patch management • How to gather intelligence on a specific dark web threat actor

Education Seminars	
Silobreaker **How to align cyber and geopolitical intelligence to navigate global risks** **Lukas Vaivuckas,** Solutions Consultant, Silobreaker & **David Hunt,** Senior Product Manager, Silobreaker	In today's volatile global landscape, the convergence of geopolitical and cyber-threats creates complex challenges for organisations worldwide. Understanding how these issues intersect is essential for threat intelligence teams, who are tasked with helping stakeholders to anticipate risks that may disrupt operations, impact security, and affect business continuity. This talk, based on key findings from a new multi-industry study, will explore practical approaches for aligning cyber and geopolitical intelligence to navigate global risks. Attendees will learn: • Structure Priority Intelligence Requirements (PIRs) for geopolitical and cyber-risks • The value of integrating between infosecurity and geopolitical risk domains • Identify patterns and correlations between geopolitical crises and cyber-risk across industries to enhance response and resilience • Shift from reactive to proactive threat intelligence, providing stakeholders with timely insights on potential threats and impacts
Silverfort **Enhancing privileged access security: Silverfort and Microsoft AD Tiering in action** **Kev Smith,** Strategic Principal Sales Engineer – EMEA, Silverfort & **Scott Goodall,** Commercial Sales Manager UKI, Silverfort	As cyber-threats grow exponentially sophisticated, securing privileged access has become a top priority for organisations worldwide. With identity-based attacks on the rise, safeguarding privileged resources is no longer optional – it's essential. This session will explore how Silverfort, in conjunction with Microsoft AD Tiering best practices, provides a proactive defence against unauthorised access and lateral movement. Attendees will learn: • Best practices for structuring and securing privileged resources using Microsoft AD Tiering • How Silverfort's patented technology enables visibility into authentication patterns across users, machines, and service accounts • Strengthening AD Tier protection with Silverfort's Privileged Access Service and Just-In-Time access control
SOCRadar **Cyber-attacks targeting the UK** **Ali Uzun,** Senior Solutions Engineer (EMEA & UKI), SOCRadar	Ransomware attacks are a growing crisis, with cybercriminals extorting millions from businesses worldwide. This seminar explores real-world lessons from $100m ransomware cases, revealing the psychology, tactics, and strategies behind successful ransomware negotiations. Attendees will gain practical insights into managing crisis teams, understanding ransom demands, and negotiating with threat actors. By learning the art of negotiation, participants will be better equipped to minimise damage, protect their data, and turn the tables on cyber-extortionists. Attendees will learn: • Understanding ransomware threats – How ransomware groups operate and set ransom demands • Key negotiation strategies – Setting limits, verifying threats, and managing crisis communications • Tactics to reduce ransom payments – Extending negotiations, leveraging strategic offers, and psychological techniques • Post-negotiation best practices – Ensuring data recovery, reporting incidents, and strengthening future defences
Tanium **Harder, Better, Faster, Stronger** **Chris Jones,** Senior Advanced Consulting Engineer, Tanium	In this session Chris Jones, will delve into the key things organisations need to consider when building a robust cybersecurity strategy. Attendees will learn: • Cybersecurity is getting Harder. How can organisations be secure when they have less people, a larger estate and a larger attack surface? • How can organisations make it Better? The importance of people, technology and process • Why you need your data Faster? And why real time data measured in milliseconds is imperative • How to make your organisation Stronger with visibility, control, and remediation

Education Seminars	
Varonis **Connecting data security to the identity fabric** **Dave Philpotts,** Sales Engineer, Varonis	Data and access events are tied intrinsically to identity. Security teams monitor data access and administration by focusing on the 'who?' of an action, including non-human identities like machine and service accounts. That's why effective data security platforms must intrinsically incorporate the identity context, otherwise known as the identity fabric. Attendees will learn: • How cyber-attacks start with an identity exploit and end with data compromise • Why identity posture is important for data security • Where ITDR can stop breaches before it's too late • What measures to take in integrating identity and data
Varonis **CISO secrets: Strengthening cyber-resilience in 2025** **Andy Dreier,** Sales Engineer, Varonis	In 2025 we're already seeing an increase in AI-driven attacks, alongside the hidden risks of cloud adoption and ever-present insider threats. It's becoming harder than ever to ensure your data is secure. In this session, we'll explore how a data-centric, identity-first approach, combined with automation and DSPM, can advance your security posture and help your organisation stay ahead of these emerging threats. We'll share the security playbook created from conversations with top CISOs and other cybersecurity leaders across manufacturing, finance, and other industries. Attendees will learn: • Discover where top CISOs are focusing their efforts in 2025 • Understand how hackers are logging in, not breaking in • Feel prepared to tackle AI security safely and securely • Better understand IaaS and SaaS security to strengthen your cloud data defences • How to use automation to improve your security posture and combat threats