

Post event report



The 18th e-Crime & Cybersecurity Mid-Year Summit

15th October 2026 | London, UK

Principal Sponsor



Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsors



Executive Roundtable Sponsors



Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars

Key themes	Speakers
AI and quantum	Michael Adjei, Director, Systems Engineering, Illumio
Identity, authority, and control for non-human actors	Wisdom Aveh, Head of Information Security & Data Protection Officer, Kurt Geiger
Data protection and leakage risks	Tim Ayling, Vice President – Cyber Solutions Specialists, Thales
AI anti-phishing and social engineering defences	James Beary, Sales Director, CybSafe
Who needs to be quantum-ready?	Tom Beshaw, Head of Security Operations & Threat Management, Johnson Matthey
Integrity and the AI-enabled supply chain	Simon Brady, AKJ Associates
Intelligent Threat Detection	Niall Browne, CEO and Co-founder, AIBound
Building better security	Richard Cassidy, International CISO, Rubrik
Making the best use of threat intelligence	Jonathan Dean, Enterprise Architect – Operational Technology, Southern Water
Security posture management	Alexander Decarne, Sr Product Marketing Manager, Threat Protection, Mimecast
Improving continuous attack surface discovery	Andrew Dreier, Manager of Sales Engineering, Varonis
The power of automation	Ian Dutton, EMEA Sales Engineering Lead, LMNTRIX
Best practice fundamentals	Lee Elliott, Director of Solutions Engineering, BeyondTrust
Achieving visibility across ecosystems	Rob FitzSimons, Sales Engineer, Huntress
Transitioning OT to the Cloud?	Rob Flanders, Head of Threat and Incident Response, BAE Systems
Defending against the latest ransomware variants	Barri-Jon Graham, Head of Cyber Threat Intelligence, Beazley
Securing the basics	Rob Gupta, Founder and CEO, ConnectProtect
Why zero trust, isolation and segmentation are key	Polina Korosteleva, Principal Security Architect, Trainline
Dealing with regulations	Etay Maor, VP Threat Intelligence and Founding Member of Cato CTRL, Cato Networks
Who attended?	Ed Maunders, Security Solutions Engineer, Sublime Security
	John McLoughlin, Group CEO, J2 Software
	John McNamee, Sales Manager, ThreatLocker
	Richard Meeus, Senior Director Security Technology and Strategy, EMEA, Akamai
	Alistair Mills, Director, Sales Engineering, Proofpoint
	Faisal Misle, Senior Lead Engineer, Customer Success, Red Sift
	Chris Morris, Senior Sales Engineer, Vega
	Raam Ratnam, Managing Director, EMEA Corporate Ratings, London, S&P Global
	Soraya Viloría Montes de Oca, Group Information Security Officer, Harvey Nichols
	Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England
	Scott Shields, Enterprise Sales Engineer, Delinea
	Leroy Stanford, Director of Cyber Security, Ocado Group
	Chris Vaughan, Security Engineer, Sublime Security
	Katie Wood, Information Security Architect, Bibby Financial Services Limited

Agenda	
08:00	Breakfast networking and registration
08:50	Chairman's welcome
09:00	A volatile world: The cyber-threat landscape in late 2026 Rob Flanders , Head of Threat and Incident Response, BAE Systems • New conflicts: How novel techniques are enabling adversaries in conflict. • New threats: How AI models are both improving threat actors capabilities, and rogue agentic systems are committing their own cyber-attacks. • The future of cyber: With AI dominating the narrative, where does cybersecurity go next?
09:20	Trust, then autonomy: A new framework for evaluating agentic AI in security Chris Vaughan , Security Engineer, Sublime Security Over the past 18 months, the security industry has sprinted from 'AI-assisted' to 'autonomous'. At most large scale industry conferences you attend in 2026, the show floors are almost entirely dedicated to agentic AI, yet the evaluation rigour applied to those products has barely changed. This talk will cover: • How to identify the gap between the autonomy a vendor markets and the autonomy they actually deliver, and why that gap is more dangerous in security than anywhere else. • A practical autonomy framework for security AI (the equivalent of SAE levels) and why advancing from Level 1 to Level 4 is a trust relationship between vendor and customer, built on transparency, explainability, and auditability, rather than a product roadmap. • What rigorous AI evaluation actually looks like: benchmark design, test set construction, and why a vendor who can only show results (not methodology) is telling you something important. • Six questions to ask any security vendor that claims to have autonomous AI, which cannot be answered with marketing speak.
09:40	A modern identity security story: What one real breach teaches us about standing privilege Lee Elliott , Director of Solutions Engineering, BeyondTrust • In this session, BeyondTrust's Lee Elliot walks you through a real supply chain breach involving two companies, six hops, and three identity classes. We will show how standing privilege, not exploits or malware, let attackers move from a compromised laptop to full production access, and how that risk could have been eliminated with zero standing privilege. • See how a single compromised endpoint escalated into a six-hop breach across two companies without any exploit, malware, or privilege escalation. Everything worked as designed. • Learn why standing privilege, not identity type, is the real attack surface, whether the identity is human, machine, or AI • Understand the difficult questions you need to ask to assess your identity and access posture. • Learn how to reach zero standing privilege with the visibility, intelligence, and enforcement needed to shrink your identity attack surface.
10:00	PANEL DISCUSSION Capacity or efficiency – what's the real issue in cyber-defence? Simon Brady , Event Chairman, Moderator; Tom Beshaw , Head of Security Operations & Threat Management, Johnson Matthey; Leroy Stanford , Director of Cyber Security, Ocado Group; Chris Morris , Senior Sales Engineer, Vega • For years, cybersecurity has been framed as a capacity challenge: more threats, more alerts, more tools, and never enough people or budget. But what if the real constraint isn't capacity at all? What if organisations are failing to get the most from the people, platforms, and data they already have? • Are security teams truly capacity constrained, or is operational inefficiency the bigger barrier to improving cyber-resilience? • Where is the greatest source of inefficiency today – people, processes, technology, or fragmented data? • How should organisations measure efficiency in cyber-defence, and what metrics best demonstrate a meaningful reduction in cyber-risk? • If you had one strategic investment over the next three years, would you prioritise increasing capacity or improving efficiency – and why?

Agenda

10:20	Education Seminars Session 1										
	<table> <tr> <td>AIBound</td><td> From the front lines: A five-time CISO's 5 lessons – and how AI rewrites the rules Niall Browne, CEO and Co-founder, AIBound </td></tr> <tr> <td>Cato Networks</td><td> Humans are the weakest link? Think again Etay Maor, VP Threat Intelligence and Founding Member of Cato CTRL, Cato Networks </td></tr> <tr> <td>OneSpan</td><td> Own, outsource, automate, eliminate: A framework for a successful passwordless implementation Marta Góral, Head of Partner Sales, UK&I, OneSpan & John Gilbert, Director, Red Lodge Consulting Ltd </td></tr> <tr> <td>Proofpoint</td><td> The agentic enterprise: Securing humans, data, and AI Alistair Mills, Director, Sales Engineering, Proofpoint </td></tr> <tr> <td>Varonis</td><td> Built, deployed, compliant: How to map your AI and avoid regulatory fines Andrew Dreier, Manager of Sales Engineering, Varonis </td></tr> </table>	AIBound	From the front lines: A five-time CISO's 5 lessons – and how AI rewrites the rules Niall Browne , CEO and Co-founder, AIBound	Cato Networks	Humans are the weakest link? Think again Etay Maor , VP Threat Intelligence and Founding Member of Cato CTRL, Cato Networks	OneSpan	Own, outsource, automate, eliminate: A framework for a successful passwordless implementation Marta Góral , Head of Partner Sales, UK&I, OneSpan & John Gilbert , Director, Red Lodge Consulting Ltd	Proofpoint	The agentic enterprise: Securing humans, data, and AI Alistair Mills , Director, Sales Engineering, Proofpoint	Varonis	Built, deployed, compliant: How to map your AI and avoid regulatory fines Andrew Dreier , Manager of Sales Engineering, Varonis
AIBound	From the front lines: A five-time CISO's 5 lessons – and how AI rewrites the rules Niall Browne , CEO and Co-founder, AIBound										
Cato Networks	Humans are the weakest link? Think again Etay Maor , VP Threat Intelligence and Founding Member of Cato CTRL, Cato Networks										
OneSpan	Own, outsource, automate, eliminate: A framework for a successful passwordless implementation Marta Góral , Head of Partner Sales, UK&I, OneSpan & John Gilbert , Director, Red Lodge Consulting Ltd										
Proofpoint	The agentic enterprise: Securing humans, data, and AI Alistair Mills , Director, Sales Engineering, Proofpoint										
Varonis	Built, deployed, compliant: How to map your AI and avoid regulatory fines Andrew Dreier , Manager of Sales Engineering, Varonis										
11:00	Networking break										
11:30	You have a gap in your intelligence programme										
	Barri-Jon Graham, Head of Cyber Threat Intelligence, Beazley - Find your gap: Diagnose which of three gaps (value, integration or trust) is holding your threat intelligence back, using one test question for each. - Turn intelligence into action: Learn how to anchor CTI to requirements the business sets and land it where it changes something (the risk register, vulnerability prioritisation and investment decisions). - Know what to believe: Recognise intelligence you can rely on, including how confidence should be expressed, and measure your programme by decisions changed instead of reports produced.										
11:50	Agentic AI, business psychology and the new resilience risk										
	Richard Cassidy, International CISO, Rubrik - As agentic AI enters live enterprise environments with minimal human oversight, autonomous decision-making is rapidly outpacing traditional controls – exposing critical vulnerabilities across data governance, supply chains, and operational accountability. - In this cybersecurity event presentation, Rubrik's EMEA CISO, Richard Cassidy, unpacks what 'going rogue' actually looks like in real-world AI deployments. - Attend this session to gain practical strategies for detecting, containing, and governing machine-speed AI risks before operational control slips away.										
12:10	Meet your rogue agents										
	Scott Shields, Enterprise Sales Engineer, Delinea - Every headline AI agent incident this year shares the same root cause: the database deleted in nine seconds, the outage from an agent left to 'fix' its own problem, the AI that kept finding new ways to act after being shut down. Nothing was hacked. Nothing broke. Every action was taken with credentials the agent was, technically, allowed to use. - The uncomfortable truth for security leaders is not that agents might go rogue, its recognising they are rogue by design without appropriate controls. - This reframes agentic AI as an identity and access problem, not a model-safety one. - This session will cover some real-world learnings from the field and offer some practical insights to help you securely prepare for the agentic era.										
12:30	Empowering cyber-defence: Fighting against the AI bot threat										
	Tim Ayling, Vice President – Cyber Solutions Specialists, Thales - Artificial intelligence is revolutionising the cybersecurity landscape, enabling organisations to detect threats faster, respond to incidents more effectively, and stay one step ahead of adversaries. - Join Thales for an in-depth exploration of how AI solutions are shaping the future of cyber-defence. - Our experts will examine real-world examples, highlight the benefits and challenges of integrating AI into existing security ecosystems, and showcase the latest AI advancements from Thales that deliver enhanced threat detection and automated response. - Learn how you can leverage AI to proactively secure your organisation's digital assets and adapt to the rapidly evolving threat landscape. - This interactive session will provide valuable insights for cybersecurity leaders, IT professionals, and anyone interested in building AI-powered resilience.										

Agenda

12:50 Education Seminars | Session 2

Akamai	Smaller surfaces. Smaller spend. Controlled agents. Controlled runtimes Richard Meeus , Senior Director Security Technology and Strategy, EMEA, Akamai
J2 Software	Million dollar conversation: What happens when the criminal isn't breaking into the conversation, they're already in it? John Mc Loughlin , Group CEO, J2 Software
LMNTRIX	When the attacker is an AI agent Ian Dutton , EMEA Sales Engineering Lead, LMNTRIX
Mimecast	AI agents are the ultimate insiders: Securing AI and the humans behind it Alexander Decarne , Sr Product Marketing Manager, Threat Protection, Mimecast
Red Sift	From secure email to brand recognition with BIMl Faisal Misle , Senior Lead Engineer, Customer Success, Red Sift

13:30 Lunch and networking

14:30 FIRESIDE CHAT: Cybersecurity at a tipping point – the future of the security stack

- Simon Brady**, Event Chairman (Moderator); **Polina Korosteleva**, Principal Security Architect, Trainline;
Jonathan Dean, Enterprise Architect – Operational Technology, Southern Water
- Are the largest security platforms pulling away, and can smaller vendors keep pace with the speed and investment AI demands?
 - Are large organisations moving from best-of-breed point solutions towards fewer, broader platforms? Are we at a genuine tipping point?
 - How large organisations buy security technology today: What matters when evaluating new technology: innovation, integration, resilience, cost and vendor longevity?
 - In an AI-driven world, where will specialist vendors still have an edge, and what will the security stack of the future look like?

15:00 Evolving security in a changing threat landscape

- Rob FitzSimons**, Sales Engineer, Huntress
- As we continue to see, organisations continue to be targeted by attackers who do not need to break in, they simply log in using stolen credentials, compromised identities, or trusted tools.
 - This session explores how organisations can move beyond alert fatigue and respond to the threats that matter most.
 - We will discuss the modern attack chain, the importance of detecting initial access and lateral movement early, and how human-led threat hunting and security posture management can help protect organisations and strengthen resilience around the clock.

15:20 Anti-heroes! Why AI goes rogue

- Michael Adjei**, Director, Systems Engineering, Illumio
- We are now in the agentic AI era, but what happens when your supposedly trusted agent turns rogue? Why does that even happen? And more importantly, could your organisation be the next victim?
 - The misalignment of increasingly capable AI models continues to be a big challenge for the major AI vendors.
 - This means that the consumer organisations who are using these models could potentially be harbouring dangerous rogue agents deep inside their corporate networks – and the risk becomes more evident with each new reported frontier release.
 - So, in this session, Michael Adjei, Director of Systems Engineering at the breach containment company, Illumio, will take attendees through the principles of: why AI agents go rogue; how rogue AI is amplifying existing foundational cyber-problems; what it means for cyber- and business-resilience; and rethinking defence in-depth for this new agentic AI era.

15:40 Zero Trust controls at the endpoint

- John McNamee**, Sales Manager, 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.

Agenda

15:45	Education Seminars Session 3	
	ConnectProtect	You don't need more security tools. You need more control Rob Gupta , Founder and CEO, ConnectProtect
	CybSafe	Key findings from The Annual Cybersecurity Attitudes and Behaviours Report 2025/26 James Beary , Sales Director, CybSafe
	Sublime Security	Inside the inbox: Anatomy of an email attack Chris Vaughan , Security Engineer & Ed Maunders , Security Solutions Engineer, Sublime Security
16:20	Networking break	
16:40	PANEL DISCUSSION	The new security baseline: People, platforms and priorities
	Simon Brady, AKJ Associates, Moderator; Katie Wood, Information Security Architect, Bibby Financial Services Limited; Soraya Viloría Montes de Oca, Group Information Security Officer, Harvey Nichols; Raam Ratnam, Managing Director, EMEA Corporate Ratings, London, S&P Global; Wisdom Aveh, Head of Information Security & Data Protection Officer, Kurt Geiger • Which cybersecurity capabilities must organisations retain in-house, and which can be safely outsourced or automated without undermining resilience? • What does a minimum viable security technology stack look like in 2026, and which tools, controls, and processes no longer justify the operational burden they create? • What framework should CISOs use to decide which risks to mitigate, transfer, automate, or formally accept when security demand exceeds available capacity?	
17:10	Rise of autonomous attacks (live Mythos-style hack)	
	Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England • See how autonomous AI agents are now running the recon and exploitation phases of real-world attacks. and what that means for boards, CISOs, and red teams in 2026. • A first-hand look at how agentic offensive AI works in practice, driven by intent, not step-by-step instruction. • See AI agent run reconnaissance against a controlled target, identify exploitable assets, and demonstrate the early stages of a kill chain in real time. • A walk through real-world findings from recent engagements including critical vulnerabilities discovered by AI agents that automated scanners had missed for over 18 years. • What defenders need to know: Why traditional, control-based security models are structurally insufficient against goal-driven autonomous attackers, and the three specific actions every CISO should be taking before this becomes the default attacker model.	
17:30	Chairman's closing remarks	
17:35	Drinks reception & networking, kindly sponsored by Vega.io	
18:30	End of conference	

Education Seminars

AlBound

From the front lines: A five-time CISO's 5 lessons – and how AI rewrites the rules

Niall Browne, CEO and Co-Founder, AlBound

Niall Browne – five-time Global CISO (Palo Alto Networks, Workday) turned AI security founder and CEO of AlBound – has spent his career in the trenches, protecting the world's most critical enterprise infrastructure and partnering with law enforcement on cyber threats. Now he distills the five hard-won lessons from thousands of real-world industry security incidents that separate resilient organisations from the breached – and confronts how AI rewrites the rules: attacks that are faster, smarter, stealthier, no longer bound by scale, and able to exploit zero-days across many targets at once. A rare view from someone who has both defended Fortune 500 infrastructure and built AI security from the ground up.

Attendees will learn:

- The top five ways hackers breach organisations today, from a former Palo Alto Networks and Workday CISO with 25 years in security.
- How AI lets attackers move faster and deeper into your systems, and why traditional defences miss AI
- Hard-won lessons from thousands of real-world incidents you can apply now to defend against AI-driven attacks.

Akamai

Smaller surfaces. Smaller spend. Controlled agents. Controlled runtimes

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

This session will explore strategic ways to optimise your defences for rapid financial return, with the potential to achieve full payback in as little as six months. Discover how reducing your attack surface can strengthen security while lowering costs. You'll also learn how modern Microsegmentation can enable more controlled agent and runtime deployment, isolating critical workloads to contain breaches faster and accelerate incident response.

Attendees will learn:

- Smaller surfaces, smaller spend. Discover how reducing your attack surface doesn't require bigger budgets but actually lowers them. In this session, you'll learn practical, proven ways to strengthen your security posture while actively cutting costs.
- Rapid financial return. Learn how optimising your defences can yield maximum economic efficiency, giving your organisation the potential to see a full payback on your security investment in as little as six months.
- Controlled agent and runtime deployment. Explore how modern microsegmentation isolates critical workloads and applications to contain breaches faster and accelerate incident response times.

Cato Networks

Humans are the weakest link? Think again

Etay Maor, VP Threat Intelligence and Founding Member of Cato CTRL, Cato Networks

Cybersecurity has long treated humans as the weakest link - people make mistakes, are easy to socially engineer, are slow to change behaviour, and pose insider-threat risk. In this session, Etay Maor (VP of Threat Intelligence at Cato Networks and founding member of Cato CTRL) argues those same four weaknesses now apply to AI and AI agents - making AI the new weakest link in the enterprise. Drawing on real attacks, live demonstrations, and intelligence gathered from dark web and criminal forums, he shows how attackers are weaponising AI systems and agents, exposing risks most security teams can't yet see.

Attendees will learn:

- The 'weakest link' framing is shifting: the same reasons humans were called insecure now describe the risks AI agents introduce into the enterprise
- Live demonstrations of real attacks and exploitation techniques against AI agents - not just theory
- Intelligence straight from the dark web and criminal forums on how threat actors are actually talking about and using AI
- 'Shadow AI' is already inside most organisations - employees unknowingly leak confidential data into public AI tools, and security teams often have no visibility into it
- A challenge to rethink current AI agent security approaches, with practical implications for how enterprises should govern and monitor agentic AI use

Education Seminars

ConnectProtect

You don't need more security tools. You need more control.

Rob Gupta, Founder and CEO, ConnectProtect

Security teams are under more pressure than ever: threats are increasing, budgets and resources are stretched, compliance expectations are growing, and organisations are managing an increasingly complex mix of tools, alerts and systems. Adding more technology doesn't necessarily create more control, it can create more complexity. This session explores a smarter, more practical approach to security: getting greater value from the tools and investments you already have, reducing operational pressure, and creating a clearer, more manageable security model.

Attendees will learn:

- Why security complexity keeps growing and how disconnected tools, limited resources and increasing accountability can make risk harder to manage.
- How to get more from your existing security investments by bringing data together, correlating and prioritising threats, and combining automation, AI and human expertise.
- How to move from reactive to proactive security, with 24x7x365 monitoring and hands-on support that helps take pressure away from internal technical teams.
- How to make security value more visible to the business, including demonstrating ROI, supporting compliance and creating more predictable security costs.

CybSafe

Key findings from The Annual Cybersecurity Attitudes and Behaviours Report 2025/26

James Beary, Sales Director, CybSafe

Join us for a review of the key findings of the latest (sixth, to be exact) 'Oh, Behave!' report.

Attendees will learn:

- Global snapshot: We'll present a global snapshot of people's cybersecurity attitudes and behaviours.
- Mindsets & motivations: What do people really think about cybersecurity, and what keeps them up at night? We'll explore who they rely on for protection and where they place the responsibility.
- The AI challenge: AI use has exploded, but training hasn't. People are more confident, but also more vulnerable. In a world of shadow AI and deepfake scams, we'll discuss how to bridge the knowing-doing gap.

J2 Software

Million dollar conversation: What happens when the criminal isn't breaking into the conversation, they're already in it?

John Mc Loughlin, Group CEO, J2 Software

In this 30-minute session, John Mc Loughlin, Group CEO of J2 Software, will take the audience inside two real-world attacks where criminals quietly inserted themselves into legitimate business conversations that cost the businesses millions. This is a story of deception, impersonation and massive losses. John will show how thinking you are safe with security tools can hurt you. The story will unpack a crypto loss of \$1.6 Million in one case and \$4 million and personal losses for directors in the second. The criminals were talking to both parties, and nobody knew until after the money was gone.

Attendees will learn:

- John will reveal how the attacks unfolded, the missed opportunities that could have exposed the criminals earlier, and how even two legal firms conducting due diligence in the second case were themselves deceived.
- This is not a session about another security service. This is about trust, identity, human behaviour, visibility and what happens when criminals become an invisible participant in a legitimate business conversation.
- Who is really in your next million-dollar conversation?

LMNTRIX

When the attacker is an AI agent

Ian Dutton, EMEA Sales Engineering Lead, LMNTRIX

AI Agents have become the new cyber attackers. AI used to be a productivity tool which the human adversary operated, phishing became better, malware was easily created, reconnaissance was summarised and social engineering scripts were produced. Now the roles have reversed, AI which used to advise the human has now become the operator, carrying out real end to end intrusions at machine speed with minimal human input.

Attendees will learn:

- How AI-powered attacks are evolving.
- What real campaigns look like.
- Real-world examples of AI agents in action over the last 12 months.
- How to effectively detect, investigate and contain these threats.

Education Seminars

Mimecast

AI agents are the ultimate insiders: Securing AI and the humans behind it

Alexander Decarne, Sr Product Marketing Manager, Threat Protection, Mimecast

Over a billion AI agents will operate inside enterprises by 2029, acting for every employee: accessing data, executing tasks, and making decisions. The agent is no longer a tool used by an insider – it has become the insider. The same agent, deployed by two different people, isn't the same risk. This session reframes agentic AI as an insider problem, covering ways to manage this risk: attributing each agent to its human, and securing both as one.

Attendees will learn:

- Why AI agents should be treated as an emerging insider risk.
- How the same AI agent can pose different risks depending on who deploys it.
- How to secure the human and their AI agent as a single identity.

OneSpan

Own, outsource, automate, eliminate: A framework for a successful passwordless implementation

Marta Góral, Head of Partner Sales, UK&I, OneSpan & John Gilbert, Director, Red Lodge Consulting Ltd

Security leaders are increasingly being made aware that they can't own everything, without unlimited resources, they have to make hard capacity calls. Passwordless authentication is a perfect example; everyone agrees FIDO2 is now mandatory, but nobody has the internal capacity to run hardware logistics, credential lifecycle, and recovery workflows at enterprise scale. That's not a technology gap, it's an operational capacity gap and it's exactly the kind of thing the eCrime Summit's own framework says should be outsourced.

Attendees will learn:

- In this session we will examine what must we own, what can we safely outsource, what should be automated, and what should we stop doing in relation to deploying phishing resistant authentication in the enterprise.
- We'll highlight how OneSpan's FIDO + CMS platform delivers the security outcome (AAL3, phishing-resistant), Digipass as a Service delivers the capacity outcome (fully managed, so the CISO's team never has to build or staff for it) and how together, they let a CISO check the box marked 'delivered' rather than 'in progress'.

Proofpoint

The Agentic Enterprise: Securing humans, data, and AI

Alistair Mills, Director, Sales Engineering, Proofpoint

The Agentic Enterprise: Securing Humans, Data, and AI explores how the rapid adoption of AI tools and autonomous agents is reshaping the enterprise security landscape. As humans and AI increasingly work side by side, agents are gaining access to sensitive data, systems and business processes with privileges approaching those of employees – but often without equivalent oversight. The session examines three emerging risk vectors: AI-generated threats that make attacks cheaper and easier to scale, over-privileged AI that can expose sensitive enterprise data, and runtime risk when autonomous agents act beyond intended boundaries. It then outlines a unified approach to securing the 'agentic workspace,' bringing collaboration, data and AI security together rather than treating them as separate problems.

Attendees will learn:

- Control what AI can access and reuse. Apply least-privilege principles to AI by default and understand what sensitive data existing tools and agents can already reach.
- Treat email, collaboration and AI as one attack surface. AI is accelerating familiar threats and allowing attacks to move across channels, making connected detection and protection increasingly important.
- Treat every AI agent like an insider. Agents need clearly defined identities, permissions, behavioural boundaries and accountability – just as employees do.
- Start with visibility and audit ability. Organisations should know which AI tools and agents are operating, who approved them, what data they can access and whether their actions can be reconstructed through an audit trail.

Education Seminars

Red Sift

From secure email to brand recognition with BIMl

Faisal Misle, Senior Lead Engineer, Customer Success, Red Sift

A brand's logo in the inbox is one of the first trust signals for a recipient. In this seminar, Red Sift breaks down Brand Indicators for Message Identification (BIMl), what it is, the authentication protocols behind it, and how AI shortens the path.

BIMl displays your verified logo on authenticated email, but it isn't something you just switch on. SPF, DKIM and DMARC need to be working together first, and a single weak link can hold the whole thing back.

Attendees will learn:

- The impact of BIMl and why it's a mark of trust
- How SPF, DKIM and DMARC interact as the foundation
- What happens when one of those protocols breaks
- The steps to adopting BIMl, simplified

Sublime Security

Inside the Inbox: Anatomy of an email attack

Chris Vaughan, Security Engineer, Sublime Security & **Ed Maunders**, Security Solutions Engineer, Sublime Security

Join Sublime for a live walkthrough of a real life attack discovery, the reasoning behind the verdict, and detections deployed in response.

You'll see Sublime's AI agents, ASA (Autonomous Security Analyst) and ADÉ (Autonomous Detection Engineer) in real time, doing what they are designed and deployed to do: how ASA triages user reported email end-to-end, and how ADÉ generates and deploys a new, org-specific detection in response to a real threat.

Attendees will learn:

- See a live walkthrough of Sublime's operational experience
- How ASA triages user reported email end-to-end
- How ADÉ generates and deploys new, org-specific detections in response to new threats
- There is an open Q&A, bring your hardest example

Varonis

Built, deployed, compliant: How to map your AI and avoid regulatory fines

Andrew Dreier, Manager of Sales Engineering, Varonis

As AI adoption accelerates across every part of the business, compliance teams are facing increased pressure to understand where AI is being used, what data it can access, and how to meet evolving regulatory requirements. With the EU AI Act and other global AI regulations taking effect, organisations need a clear view of both sanctioned and shadow AI to reduce risk and demonstrate compliance. Join this session to learn how to discover, assess, and govern AI across your environment with confidence.

Attendees will learn:

- The latest EU AI Act requirements and key compliance deadlines organisations need to prepare for.
- How to uncover sanctioned, custom-built, and shadow AI applications across your organisation.
- Practical ways to identify AI-related risks and generate the evidence needed for regulatory compliance.
- Why a strong, consistent data security strategy is the foundation for secure and compliant AI adoption.