Post event report

The 17th e-Crime & Cybersecurity Mid-Year Summit

16th October 2025 | London, UK

Principal Sponsor

BeyondTrust

Strategic Sponsors

CultureAI

illumio

mimecast

proofpoint

Quorum Cyber

SEARCHLIGHT CYBER

Silverfort

THREATLOCKER

Education Seminar Sponsors

Abnormal

Akamai

brookcourt
A Shearwater Group plc Company

CONTRAST SECURITY

CYBSAFE

goldilock

IRONSCALES

OneSpan

RED SIFT

REVERSEC

RISK LEDGER

rubrik

sectona

VARONIS

"The event was excellent, well organised and provided valuable insights into a wide range of topics relevant to the current and emerging cybersecurity threats along with practical solutions for threat countermeasures."
Head of Infrastructure Management, Dnata Travel Group

"Really enjoyed yesterday's event – plenty of thought-provoking insights and standout presentations, particularly from OVO and the Virgin Media O2 Group. From an OT perspective, several sponsors offered valuable contributions, especially around Privileged Access Management. The behavioural analysis sessions were especially insightful, and it was great to connect with fellow professionals across the cyber-domain."
Senior Operations – SCADA, IT & OT, Scottish Power

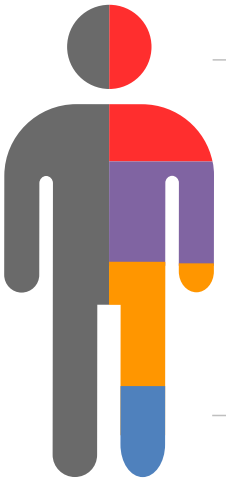
"It is my favourite of all the events I attend and really loved some of the speakers and sessions so thank you!"
Cyber Security Architect, Imperial College London

Inside this report:

Key themes

- Making the best use of threat intelligence
- Dealing with regulations
- Security Posture Management
- Improving continuous attack surface discovery
- The power of automation
- Adversary simulation and behavioural analysis
- Achieving visibility across ecosystems
- Transitioning OT to the Cloud?
- Defending against the latest ransomware variants
- OT and the regulations
- Why zero trust, isolation and segmentation are key
- Pen testing for OT / SCADA

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

Rob Ainscough, Chief Identity Security Advisor
Silverfort

Donato Capitella, Principal Security Consultant
Reversec

Federico Charosky, Founder & CEO
Quorum Cyber

Steve Davies, Head of Cyber Security
DLA Piper

Suzie Dobrontei, Behavioural Scientist
CybSafe

Dr. Marina Egea, Cybersecurity Senior Director
Santander UK

Lee Elliott,
Senior Director of Solutions Engineering
BeyondTrust

Rob Elsey, Chief Digital and Information Officer
Co-op

John Flatley, Solutions Engineer
Abnormal AI

Khetan Gajjar, EMEA CTO
Mimecast

John Gilbert, Director Red Lodge Consulting
OneSpan

Simon Goldsmith,
Director of Information Security
OVO Energy

Michael Hiscock, Solution Engineer
Sectona

Justin Kuruvilla, Chief Cyber Security Strategist
Risk Ledger

Nadim Lahoud, SVP Operations
Red Sift

Charlie Mather, Commercial Account Executive
Ironscales

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

Alistair Mills, Director, Sales Engineering
Proofpoint

Ed Morgan, GTM Technical Lead EMEA & APJ
Rubrik

Mark Pearce, Head of Global Sales & Channel
Goldilock

Ian Perry, Head of Sales Engineering
Searchlight Cyber

Sam Rea,
Head of Enterprise Security Architecture
Bupa Group

Tom Rossdale, Sales Engineer Director,
Varonis

Oliver Simonnet, Lead Cyber Security Researcher
CultureAI

Joe Tidy, Reporter, Presenter & Author
BBC

Lynette Webber, Head of Security Governance, Risk and Compliance
Virgin Media O2

John Wood, Senior Regional Sales Manager
Contrast Security

Agenda

08:00 Breakfast networking

08:50 Chair's welcome

09:00 **Technology as a squid that lost its shell**

Simon Goldsmith, Director of Information Security, OVO Energy

- Discover why the traditional 'fortress' model of cybersecurity failed in our cloud-native, interconnected world
- Learn from Jurassic squid how to evolve beyond a rigid perimeter by developing three dynamic capabilities
- Explore a practical blueprint for this evolution, redefining what we protect (from 'people' to 'identities') and splitting our response into two distinct, high-velocity workflows for attacks and weaknesses
- Understand how to reset your operating model, transforming security from a reactive gatekeeper into a proactive enabler that builds 'paved roads' to make the secure way the easy way

09:20 **AI-powered cyber-threats: The role of identity-centric strategies in modern cybersecurity**

Lee Elliott, Senior Director of Solutions Engineering, BeyondTrust

- Understand how AI is transforming the threat landscape: Gain insights into how cybercriminals are using AI to automate attacks, craft realistic phishing campaigns, and bypass traditional detection methods
- Learn why identity is a critical line of defence: Discover how identity-focused access management can protect privileged accounts and minimise risks tied to identity-based attacks
- Explore practical strategies to strengthen cyber-resilience: Leave with actionable guidance on implementing AI-driven defences and building a comprehensive cybersecurity strategy that addresses today's fast-evolving threat vectors

09:40 **Unified human risk management: Connecting the dots between technology, people, and data**

Khetan Gajjar, EMEA CTO, Mimecast

- Explore how a unified human risk management (HRM) strategy can bridge the gap between external threats and internal vulnerabilities
- Discover actionable insights to strengthen your organisation's cyber-resilience by leveraging cutting-edge AI, automation, and contextual education to reduce risks and streamline security operations
- Demonstrate how they can integrate email security with insider risk management to protect sensitive data, ensure compliance across collaboration platforms, and proactively educate employees to foster a culture of cyber-awareness
- Walk away with strategies to simplify operations, minimise incident response times, and stay ahead of emerging threats

10:00 **Enterprise security architecture: Huh? What's that?**

Sam Rea, Head of Enterprise Security Architecture, Bupa Group

- The importance of an integrated enterprise security architecture (ESA) in aligning security with business goals and strategy technology planning and delivery
- Establishing a common language and reference architecture that can be used by all technology and security professionals
- Improving your organisation's security posture while aligning with industry recognised security frameworks and governance best practices
- Driving change within your organisation by building a cross-discipline community to democratise security design knowledge, improving consistency and reducing reliance on individual security SMEs

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

Akamai	Goldilock	Red Sift	Rubrik	Sectona
The AI ecosystem from bots to hackers: A look inside today's LLM exploits and the risk from AI scrapers	**Disconnect to protect, on-demand – military-grade cybersecurity for a connected world**	**Brand impersonation: Why technical controls are a CISO's best line of defence**	**Fortify your cyber-resilience with Rubrik Identity Recovery**	**From control to confidence: The new era of modern infrastructure access**
Richard Meeus, Senior Director Security Technology and Strategy, EMEA, Akamai	**Mark Pearce,** Head of Global Sales & Channel, Goldilock	**Nadim Lahoud,** SVP Operations, Red Sift	**Ed Morgan,** GTM Technical Lead EMEA & APJ, Rubrik	**Michael Hiscock,** Solution Engineer, Sectona

11:00 Networking break

11:30 **Identity as a strategic differentiator in the age of cyber-threats**

Dr. Marina Egea, Cybersecurity Senior Director, Santander UK

- The rising complexity of identity as both a business enabler and a critical organisational challenge
- Why identity situational awareness is essential to avoid misdiagnosis and guide maturity journeys
- Strengthening internal identity governance with CIAM and lessons learned
- Leveraging data and AI to turn identity into a resilience-building, threat-response advantage

11:50 **Cybersecurity in the age of Agentic AI – Human-centric security to protect against autonomous threats**

Alistair Mills, Director, Sales Engineering, Proofpoint

- This session will examine the strategic implications of Agentic AI – autonomous systems capable of making decisions and taking actions – and the new cybersecurity risks they introduce to modern enterprises
- We'll explore how Agentic AI can be leveraged by threat actors, inadvertently misused by employees, and how its autonomous nature challenges traditional security models
- Learn how to gain visibility into the deployment and behaviour of Agentic AI within your organisation, enforce responsible use policies, and educate your workforce
- Discover why a human-centric approach to cybersecurity – focused on awareness, accountability, and resilience – is essential to protecting sensitive data and maintaining trust in an increasingly autonomous digital environment

Agenda

12:10 Cyber-resilience lessons from real-world attack & defence incidents

Michael Adjei, Director, Systems Engineering, Illumio

- Walkthrough real-world incidents
- Analyse new and improved cyber-strategies to employ
- Learn how organisations can continue viable business operations after a cyber-incident
- Modern operational resilience insights for CISOs and security managers
- Learn how to implement modern cybersecurity strategies in the era of AI

12:30 New strategies for exposure management of modern infrastructure

Ian Perry, Head of Sales Engineering, Searchlight Cyber

- How the traditional perimeter has been dissolved by the realities of cloud adoption
- The theory of continuous threat exposure management (CTEM) as a new approach to your cybersecurity
- How CTEM evolves and realises the lost promise of 'attack surface management'
- Case study examples of exposure management being deployed to prevent exploitation and cyber-attacks

12:50 Education Seminars | Session 2

BeyondTrust	Contrast Security	CybSafe	OneSpan	Varonis
Beyond privileged accounts: Identity security for today's dynamic world **Lee Elliott,** Senior Director of Solutions Engineering, BeyondTrust	**Your forgotten apps are an open invitation: ADR or incident response – your choice** **John Wood,** Senior Regional Sales Manager, Contrast Security	**Key findings from The Annual Cybersecurity Attitudes and Behaviors Report 2024/25** **Suzie Dobrontei,** Behavioural Scientist, CybSafe	**A simple, old-fashioned con: How can we keep the bad guys out and limit the damage they cause?** **John Gilbert,** Director Red Lodge Consulting, OneSpan	**Shining a light on shadow AI: The hidden risk to data security** **Tom Rossdale,** Sales Engineer Director, Varonis

13:30 Lunch & networking break

14:30 FIRESIDE CHAT: Time for a reset: Why resilience is redefining risk and the role of the CISO

Simon Brady, Event Chairman (Moderator); **Lynette Webber,** Head of Security Governance, Risk and Compliance, Virgin Media O2

- Why has cyber lagged so badly behind other risk disciplines?
- If resilience is the focus, is this really the CISO's or CISOs need to reinvent themselves as risk leaders?
- What are the practical impacts of a resilience-first model on budgets, metrics, and board engagement?
- How does resilience change culture – from blame and prevention to acceptance and preparedness?
- What skills or mindsets must the next-generation CISO have to thrive as a risk leader rather than just a technologist?

15:00 The rise of AI – Innovation, exploitation and the battle for control

Oliver Simonnet, Lead Cyber Security Researcher, CultureAI

- Artificial intelligence may feel like it appeared overnight, but its roots stretch back decades, from Turing's Bombe and symbolic reasoning to neural networks, deep learning, and today's generative and agentic systems. Each milestone laid the foundation for models that now create, converse, and increasingly act on our behalf
- But here be dragons. Cybercriminals have moved quickly to weaponise AI, from WormGPT and deepfake-driven fraud to polymorphic malware and malicious agentic systems. At the same time, organisations face mounting risks from shadow AI, data leakage, compromised accounts, and poisoned models
- This talk takes a journey through AI's history and emerging threats, highlighting that just as we secured email, cloud, and SaaS, we must now secure AI. The arms race is well underway, and those who embed governance and control today will be the ones who thrive tomorrow

15:20 From reaction to resilience: A new path for privileged access

Rob Ainscough, Chief Identity Security Advisor, Silverfort

- Understand why traditional privileged access management (PAM) methods fall short in today's evolving cyber-threat landscape
- Explore a modern, identity-centric approach that builds resilience at the core – moving from reactive controls to proactive defence
- Learn about an agentless, continuous strategy for detecting and preventing privileged identity misuse in hybrid and cloud environments
- Discover how to reduce attack surfaces, enforce adaptive access policies, and gain granular visibility – without disrupting operational workflows

15:40 Education Seminars | Session 3

Abnormal AI	Ironscales	Reversec	Risk Ledger
Inbox infiltrated: One QR code, one near miss, one game-changing fix **John Flatley,** Solutions Engineer, Abnormal AI	**Transforming cybersecurity strategies to combat GenAI and deepfake threats** **Charlie Mather,** Commercial Account Executive, Ironscales	**Foundations of GenAI application security: Understanding and mitigating risks** **Donato Capitella,** Principal Security Consultant, Reversec	**Untangling the supply chain problem** **Justin Kuruvilla,** Chief Cyber Security Strategist, Risk Ledger

16:20 Networking break

16:40 Curiosity to cybercrime: The rise of teenage hackers

Joe Tidy, Reporter, Presenter & Author, BBC

- How teenage hacking has shifted from harmless exploration to organised cybercrime
- The motivations driving young hackers – money, notoriety, and criminal recruitment
- The typical journey: from gaming cheats and scams to advanced attacks

17:00 PANEL DISCUSSION Ransomware 360°: From first click to final recovery

Simon Brady, Event Chairman (Moderator); **Rob Elsey,** Chief Digital and Information Officer, Co-op;
Steve Davies, Head of Cyber Security, DLA Piper; **Joe Tidy,** Reporter, Presenter & Author, BBC;
Federico Charosky, Founder & CEO, Quorum Cyber

- What's the smartest social engineering ploy you've seen lately – and why did it work?
- When ransomware hits, where's the biggest choke point?
- Is paying ever OK – and when?
- Where's the bigger risk – your systems, your suppliers or teenage kids?
- With limited budget, do you back prevention, detection, recovery, or training?

17:30 Drinks reception & networking **Sponsored by Quorum Cyber** **18:30** Conference close

Education Seminars	
Abnormal AI **Inbox infiltrated: One QR code, one near miss, one game-changing fix** **John Flatley,** Solutions Engineer, Abnormal AI	Email continues to be the most exploited vector in cyber-attacks – now more dangerous than ever with the rise of AI-driven threats. In this session, John Flatley from Abnormal AI presents a real-world example of a novel QR code-based phishing attack that bypassed traditional security measures. The talk highlights how attackers exploit human behaviour and why legacy defences are failing. He then introduces a modern, behavioural AI approach that stops advanced threats before they cause damage. Attendees will learn: • AI is empowering attackers: Threat actors now use AI to create highly personalised and scalable email attacks that evade traditional detection methods • The human element is the weakest link: Social engineering and mobile-based credential theft tactics are specifically designed to exploit human trust and unprotected devices • Modern problems need modern defences: Abnormal's behavioural AI platform provides automated, API-based protection that adapts to evolving threats without manual rules or configurations
Akamai **The AI ecosystem from bots to hackers: A look inside today's LLM exploits and the risk from AI scrapers** **Richard Meeus,** Senior Director Security Technology and Strategy, EMEA, Akamai	AI is a much discussed topic at the moment, with varying degrees of hope, hype and hyperbole. Large language models (LLMs) are prime targets for attacks that exploit their unpredictability, including prompt injection, AI jailbreaking, data exfiltration, and model theft. LLMs themselves are scraping every piece of knowledge in existence making them an integral part of how we use the Internet, or how they will change our use of the Internet. This session will break down how these attacks work, why they are difficult to detect, and what defenders can do to stay ahead of adversaries targeting AI and LLMs. Whether you're worried about visitor decline or referral traffic-drops to your site, or you are securing customer-facing apps, internal copilots, or proprietary models, this session will equip you with the knowledge to spot – and stop – these threats and challenges. Attendees will learn: • The anatomy of prompt injection attacks and how they bypass input filters • How AI jailbreaking leads to toxic output, policy evasion, and reputational risk • Why AI-specific DoS attacks don't look like traditional DDoS • Identify the bots visiting your site to determine whether they are beneficial to you
BeyondTrust **Beyond privileged accounts: Identity security for today's dynamic world** **Lee Elliott,** Senior Director of Solutions Engineering, BeyondTrust	Even with growing budgets and stricter compliance mandates, cyber-risk is still on the rise. Identities are a top target, with attackers exploiting hidden Paths to Privilege™ to gain access. Managing elevated permissions across hybrid environments is complex, and traditional PAM tools – focused only on privileged accounts – often leave gaps. This session will look at how modern, identity-focused PAM secures all users, reduces risk, and simplifies access to keep your organisation both protected and productive. Attendees will learn: • Uncover real-world attack paths: See how threat actors bypass traditional controls by exploiting overlooked identity vectors – even beyond privileged accounts • See modern PAM in action: Learn how identity-first approaches simplify access and security across hybrid infrastructures, with live examples and use cases • Bridge security and productivity: Discover how to protect all users – not just admins – without slowing down your workforce or partners • Leave with actionable insights: Walk away with practical steps to evolve your PAM strategy and close critical gaps in your identity security posture

Education Seminars

Contrast Security

Your forgotten apps are an open invitation: ADR or incident response – your choice

John Wood, Senior Regional Sales Manager, Contrast Security

Here is the uncomfortable truth: most breaches do not start in your Tier 1 apps. They start in the forgotten corners of your estate, the expense tool, the vendor portal, the dusty middleware running on a server no one dares to touch. Attackers know this. They are not hacking your shiny new microservices; they are walking through the side door you left wide open.

This talk is a wake-up call for CISOs, AppSec leads, and anyone still pretending 'shift left' is enough. We will dismantle the myths, expose the blind spots, and show why ADR is the only control that can protect where you cannot patch, cannot test, and cannot even find the developer who wrote the code.

Fast, sharp, and slightly dangerous – this session will make you laugh, make you sweat, and leave you with a battle plan that your board will thank you for (and your attacker will hate).

Attendees will learn:

- 'Tier 1 is theatre, Tier 3 is reality.' Learn where breaches actually begin
- 'Shift left is a fantasy, runtime is reality.' Why detection and defence have to live where the code runs
- 'You have 90 days to act – or the attackers will.' A ruthless plan to deploy ADR across your long tail in one quarter

CybSafe

Key findings from The Annual Cybersecurity Attitudes and Behaviors Report 2024/25

Suzie Dobrontei, Behavioural Scientist, CybSafe

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

Attendees will learn:

- Global snapshot: We'll present a global snapshot of people's cybersecurity attitudes and behaviours, with a focus on generational differences and country comparisons
- 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

Goldilock

Disconnect to protect, on-demand – military-grade cybersecurity for a connected world

Mark Pearce, Head of Global Sales & Channel, Goldilock Secure

In today's hyperconnected world, the convergence of operational technology (OT) and information technology (IT) has created vast new vulnerabilities. Cyber-attacks on critical infrastructure from energy grids and water supplies to hospital networks and financial markets, are escalating not only in frequency but also in nation-state-level sophistication and destructive potential. Recent high-profile incidents have starkly demonstrated that the largest, most cyber-aware organisations are not 100% protected; their multi-layered, perimeter-based defences are simply proving inadequate against patient, evasive, and highly complex threats.

One truth is becoming clear: no system is truly secure while it's connected. NATO has reaffirmed a foundational cybersecurity principle; the only foolproof way to stop a breach is to eliminate the digital attack surface each time connection is not required, by disconnecting from the internet on demand. This principle forms the bedrock upon which Goldilock Secure was conceived, 'Disconnect – To Protect, on Demand'. This session explores how military-grade technology has been adapted into a practical cybersecurity control, enabling the physical disconnection of critical systems from the internet, instantly and remotely, reducing exposure and neutralising threats at the root.

Attendees will learn:

- Discover how to instantly keep your systems truly invisible to online threats and cyber-attackers, no software or complex configs needed
- Learn how to deploy a near-instant cyber kill-switch, enabling rapid containment of active threats like ransomware while ensuring uninterrupted business operations
- Understand how hardware-enforced segregation is the new gold standard for governance. You will gain the ability to meet and prove compliance with strict mandates (including NIS2, ISO 27001, and HIPAA) by generating irrefutable, physical evidence of network separation for simplified audit trails and maximum resilience

Education Seminars	
Ironscales **Transforming cybersecurity strategies to combat GenAI and deepfake threats** **Charlie Mather,** Commercial Account Executive, Ironscales	AI-driven technologies like GenAI and deepfakes are creating challenges that IT security and MSP leaders can't afford to ignore. The surge in AI-powered attacks means traditional defences used by most organisations are no longer enough. Attackers are stepping up their game, crafting hyper-realistic, personalised attacks that are nearly indistinguishable from the real thing – and it's only going to get more intense as these tools evolve. So, how do we fight back? Attendees will learn: • We will explore how to rethink your approach, using AI to combat AI and keep pace with these threats • We will also touch on how a 'red team/blue team' strategy can help you stay one step ahead, leveraging AI to anticipate future attacks, arm your defences, and proactively mitigate them
OneSpan **A simple, old-fashioned con: How can we keep the bad guys out and limit the damage they cause?** **John Gilbert,** Director Red Lodge Consulting, OneSpan	Most data breaches and ransomware incidents continue to involve compromised credentials, as AI-enabled phishing techniques become more advanced. Identity-related cyber-attacks are particularly difficult to defend against as they often occur when attackers log in using valid credentials rather than exploiting technical vulnerabilities. Cybercriminals employ social engineering to circumvent traditional multi-factor authentication, exploit vulnerabilities within helpdesk processes, and manipulate structured environments such as privileged access management (PAM) systems and service accounts. Frequently, these gaps are only discovered after an incident has occurred – often due to inadequate user validation and ineffective access governance. Employees represent both a substantial asset and a key vulnerability in this context. The current trends observed across industries such as retail, manufacturing, and telecommunications underscore the urgent need for enhanced user validation procedures and the adoption of robust, low-friction MFA solutions and the critical importance of access visibility in understanding and managing risk associated with potential account compromise. Attendees will learn: • Why, despite the $millions spent on cybersecurity, do we still fall for a 'simple old fashioned con'? • What can we do to better secure our user accounts and minimise the risk of a breach? • What are the challenges associated with modern passwordless authentication and how do we address these?
Red Sift **Brand impersonation: Why technical controls are a CISO's best line of defence** **Nadim Lahoud,** SVP Operations, Red Sift	Brand impersonation is one of the biggest cyber-risks facing CISOs today, yet it is one of the hardest threats to demonstrably mitigate. Attackers exploit multiple vectors including, domains, email, websites, social media, and even search engine manipulation – to deceive employees, customers, and partners. In this seminar, we introduce a clear framework that categorises the main forms of brand impersonation and highlight why technical controls deserve to be the first – and most cost-effective – line of defence. Participants will gain an actionable understanding of how modern security teams can assess the scope of impersonation risk, identify the right mix of controls, and deploy them with confidence. To ground these concepts, we will share real-world case studies of organisations that have successfully reduced impersonation attacks with Red Sift. Attendees will leave with both the strategic lens to communicate risk to stakeholders and the tactical guidance to strengthen their organisations against this pervasive and evolving threat. Attendees will learn: • An understanding of brand impersonation and why it is a leading cyber-risk • A framework that clearly categorises the main impersonation vectors and explains prioritising technical controls as the first line of defence • A step-by-step playbook for deploying technical controls reliably at scale, supported by automation and operational best practices • Customer case studies of organisations that have successfully solved brand impersonation challenges with Red Sift • Practical insights to both communicate the risk to executives and apply effective solutions within existing security programmes

Education Seminars	
Reversec **Foundations of GenAI application security: Understanding and mitigating risks** **Donato Capitella,** Principal Security Consultant, Reversec	GenAI applications introduce new cybersecurity risks that developers, security professionals, and architects need to address. Attackers exploit these systems primarily through prompt injection and jailbreaking, turning AI capabilities against their intended use. This session breaks down how these attacks work, where traditional security approaches fall short, and what practical strategies can mitigate these risks. Attendees will learn: • Core security challenges when integrating GenAI into software • Common attack techniques and real-world exploitation examples • What 'good' looks like: securing GenAI applications in production
Risk Ledger **Untangling the supply chain problem** **Justin Kuruvilla,** Chief Cyber Security Strategist, Risk Ledger	As cybercrime becomes more systemic, supply chain attacks are evolving from isolated breaches into network-wide crises. In this session, Justin Kuruvilla, Chief Cyber Security Strategist at Risk Ledger, unpacks why traditional third-party risk management (TPRM) is failing to keep pace with today's interconnected threat landscape. Drawing on lessons from history and real-world data from government and critical infrastructure communities, Justin explores how concentration risk, supplier dependency, and visibility gaps are creating new attack surfaces for threat actors to exploit. Attendees will learn how to move beyond static assessments toward a collaborative, network-based model of defence, one where organisations and their suppliers work together to identify vulnerabilities, share assurance, and Defend-as-One. Attendees will learn: • See the whole system, not just the supplier. Supply chain security isn't about isolated vendors – it's about understanding the interdependencies, fourth parties, and shared providers that create systemic risk • Rethink TPRM for the threat era. Traditional, survey-based risk management is too slow and siloed to counter today's fast-moving, networked attacks. Resilience requires live visibility and shared intelligence • Defend-as-One. The future of cyber-defence is collaborative. Organisations, suppliers, and regulators must work together to identify concentration risks and strengthen collective resilience across ecosystems
Rubrik **Fortify your cyber-resilience with Rubrik Identity Recovery** **Ed Morgan,** GTM Technical Lead EMEA & APJ, Rubrik	In today's dynamically evolving threat landscape, cyber-attacks are becoming increasingly sophisticated and pervasive. As attackers continually target the core identity repositories of enterprises, it has become imperative for organisations to fortify their cyber-resilience efforts by prioritising protecting their identity data. True cyber-resilience means accepting that breaches will happen. A complete cyber-resilience strategy hinges on the ability to promptly recover from security incidents and ensure the continuity of critical business operations. In this session, we will be discussing how to ensure business continuity by rapidly recovering your Microsoft Active Directory and Entra ID environments, safeguarding your identity services from cyber-attacks and operational failures. Attendees will learn: • Protect identity systems – maintain uninterrupted operations by continuously monitoring identity risks and policy violations • Detect and remediate threats – rapidly identify compromised accounts and enforce remediation or rollback actions before they disrupt access • Seamlessly recover identity systems – orchestrate fast, reliable recovery of Active Directory and Entra ID to restore critical-business operations

Education Seminars	
Sectona **From control to confidence: The new era of modern infrastructure access** **Michael Hiscock,** Solution Engineer, Sectona	Today's enterprises operate across a vast and interconnected landscape, from on-premises infrastructure and cloud platforms and third-party networks. While this diversity offers unmatched flexibility, it also introduces complex privileged access challenges that traditional PAM solutions weren't built to address. Join Sectona for an exclusive session where we unveil our modern infrastructure access approach – designed to secure every connection, everywhere, without compromising operational efficiency. Explore how Sectona brings diverse user personas together on a single, powerful platform. Attendees will learn: • Achieving unified visibility and real-time control over privileged sessions • Enforcing least privilege and regulatory compliance seamlessly across diverse infrastructures • Securing access for internal teams, remote employees, and third-party users with minimal disruption • Eliminating blind spots and mitigating risks in hybrid and multi-cloud setups
Varonis **Shining a light on shadow AI: The hidden risk to data security** **Tom Rossdale,** Sales Engineer Director, Varonis	Shadow AI occurs when employees use tools like ChatGPT or Copilot without IT's visibility or control – a trend now seen in nearly every organisation. While these tools can boost productivity, their unsanctioned or unmonitored use introduces serious risks, including data leaks, compliance violations, and loss of intellectual property. This session will reveal how shadow AI is infiltrating organisations and what you can do to regain visibility and control. Attendees will learn: • What shadow AI is, including the difference between unsanctioned and unmonitored AI, and why both are risky • Real-world consequences, such as data leakage, regulatory breaches, and exposure of sensitive information – even with popular tools like Microsoft Copilot • Why shadow AI happens, including the drivers behind its adoption and the challenges IT and security teams face • Practical steps to detect, monitor, and manage shadow AI, from technical controls to employee education and streamlined onboarding of safe AI tools