Post event report

The 16th e-Crime & Cybersecurity Mid-Year Summit

17th October 2024 | London, UK

Strategic Sponsors

HOXHUNT

Integrity360 your security in mind

mimecast

SEARCHLIGHT CYBER

SentinelOne

TANIUM

THREATLOCKER

Education Seminar Sponsors

Abnormal

BeyondTrust

CATO NETWORKS

HADRIAN

IRONSCALES

MENLO SECURITY

netwrix

RED SIFT

SILVERFORT

TENEO OPENING MINDS | Akamai

THALES

VARONIS

Networking Sponsors

CybelAngel

Fingerprint

iZOOlogic

Branding Sponsor

Metomic

"e-Crime & Cybersecurity Summit is one event which I make every effort to attend as not only does it cover topical themes presented in a bitesize & easily digestible format but also facilitates engaging with vendors and peers to discuss solutions and experience. So, I would recommend any professional involved in information risk management, cybersecurity and IT audit to attend this event."
IT Security & Risk Officer, UBS Group

"I greatly appreciated the technical insights gained from the various presenters at the e-Crime & Cybersecurity Mid-Year Summit'. The discussion topics were incredibly valuable and relevant, making it difficult to choose between the Education Seminar breakout sessions as they were all important. The only challenge was the limited time for each session, given the high quality of information being shared. I look forward to future engagements. Keep up the excellent work, team!"
IT Change Assurance Manager, Paragon Banking Group

"Thank you for another brilliant congress again yesterday."
Security Systems Administrator, Vertas Group

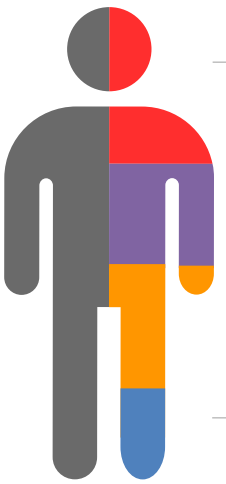
"I recently attended the e-Crime & Cybersecurity Mid-Year Summit and found it very informative. The presentations from industry leaders and security vendors were relevant and varied, and the workshops offered valuable insights. The event was well organised and beneficial for anyone in the cybersecurity field."
Head of Risk – IT Change & Assurance, Paragon Banking Group

Inside this report:

Key themes

- Maximising the utility of threat intelligence
- Personal liability for CISOs? It's here now.
- Defeating ransomware and malicious malware
- The dangers of digitalisation – securing IoT and OT ecosystems
- Why regulation will drive better cybersecurity
- Getting real about cyber-risk management
- Securing the xIoT
- Evolving incident response: lessons from the past
- AI for CISOs: the hype versus the reality
- Insuring the uninsurable?
- Developing the next generation of security leaders
- Mobile device vulnerabilities and mitigations
- Do you know your APIs?
- Is it time to rethink your Cloud strategy?
- The pros and cons of managed services
- The answer really is zero trust, isn't it?

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

Noora Ahmed-Moshe, VP of Strategy and Operations, **Hoxhunt**

Simon Ashworth, MD, Chief Analytical Officer – Insurance Ratings and Cyber Lead, **S&P Global Ratings**

Tim Ayling, VP EMEA Cyber Security Specialists, **Thales**

Brett Ayres, VP of Product, **Teneo**

Peter Batchelor, UK&I Regional Director, **Silverfort**

Mario Beccia, Deputy CIO for Cybersecurity, **NATO**

Gavin Cartwright, Tech Consulting Lead (TMT), **EY**

Paul Clark, Head of Sales, EMEA, **Ironscales**

Ian Dalby, Global Head of GRC, **A&O Shearman**

James Eason, CRA Practice Lead, **Integrity360**

Lee Elliott, Director, Solutions Engineering, **BeyondTrust**

Andy Giles, Executive Director, Head of Intelligence Integration, **JPMorgan Chase**

Parul Khedwal, Security Operations Lead, **Trainline**

Sarah Lawson, CISO & Deputy CIO, **University College London**

Seamus Lennon, Vice President of Operations for EMEA, **ThreatLocker**

Mark Logsdon, CISO, **NHS England**

Etay Maor, Chief Security Strategist, Founding Member of Cato CTRL, **Cato Networks**

Billy McDiarmid, Sr Director of Sales Engineering, **Red Sift**

Richard Meeus, EMEA Director of Security Technology and Strategy, **Akamai**

Goher Mohammad, Group Head of InfoSec, **L&Q Group**

Anthony Moillic, Field CISO, **Netwrix Corporation**

Richard Orange, Regional Vice President of EMEA, **Abnormal Security**

Dave Osler, Head of Product, **Searchlight Cyber**

Clair Phelps, CISO, **Wagestream**

William Priestley, Sales Engineer Manager, **Varonis**

Brett Raybould, Director, Solutions Engineering, **Menlo Security**

Manit Sahib, Ethical Hacker, **The Global Fund**

Al Scott, Senior Sales Engineer EMEA, **Silverfort**

Glenn Smith, Principal Sales Engineer, **Mimecast**

Prash Somaiya, CTO, **Hadrian**

Valentina Soria, Global Head of Cyber Threat Intelligence, **UBS**

Zac Warren, Chief Security Advisor, **Tanium**

Elliott Went, Senior Solutions Engineer, UKI, **SentinelOne**

Evie Wild, Information Security Officer, EMEA Region, **LBBW Bank**

Agenda

08:00 Registration and breakfast networking

08:50 Chairman's welcome

09:00 **Building an adaptive cybersecurity function**

Mario Beccia, Deputy CIO for Cybersecurity, NATO

- The threat picture and the challenge of constant adaptation
- Planning your next cybersecurity incident: Infrastructure resilience, scalability and simplification
- Embracing emerging technologies
- The changing role of the Blue Team

09:20 **Future-proofing Europe: The next era of cybersecurity?**

Zac Warren, Chief Security Advisor, Tanium

- The importance of proactive measures to protect digital assets and highlight the role of people, processes, and technology in this endeavour
- Insights into the future challenges and opportunities in cybersecurity and how organisations can effectively address them
- The growing demand for skilled cybersecurity professionals and the necessity of continuous education and training to stay ahead of cyber-threats
- The significance of implementing preventative and comprehensive strategies such as zero-trust security models to ensure compliance with regulations and standards
- The role of AI and ML in enhancing cybersecurity through real-time threat detection, predictive analysis, and automated security operations

09:40 **The complexity conundrum: Three steps to simplifying security complexity**

Elliott Went, Senior Solutions Engineer, UKI, SentinelOne

- The security complexity challenges of today
- Your complexity is leaving you vulnerable. A deep dive in today's existing threat landscape
- Simplifying the complexity: Reducing risk across endpoint, identity, cloud surfaces and more
- Simplification starts with these three key actions

10:00 **FIRESIDE CHAT: Integrating cybersecurity into mergers, IPOs, and ESG strategies**

Ian Dalby, Global Head of GRC, A&O Shearman;
Simon Ashworth, MD, Chief Analytical Officer – Insurance Ratings and Cyber Lead, S&P Global Ratings

- How do companies prioritise cybersecurity due diligence, and what specific metrics or risks are most critical, when planning a merger or IPO?
- What role do cybersecurity audits and due diligence play in the preparation phase for mergers and IPOs?
- How can companies identify and mitigate cyber-risks that could impact valuation or delay the IPO/merger process?
- How does cybersecurity intersect with ESG criteria, and why is it crucial for integrating cybersecurity practices into ESG strategies?
- How are investors and stakeholders increasingly viewing cybersecurity as a critical component of a company's ESG performance, and are current regulations effective in deterring non-compliance?
- How do you align and integrate cybersecurity practices post-merger?

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

BeyondTrust	Hadrian	Ironscales	Red Sift	Teneo & Akamai	Varonis
Hackers don't hack in – they log in. How to combat the threat of identity compromise **Lee Elliott,** Director, Solutions Engineering, BeyondTrust	**How to become proactive and stay ahead of the AI threat curve** **Prash Somaiya,** CTO, Hadrian	**Go on the offensive by merging AI and human expertise for email security** **Paul Clark,** Head of Sales, EMEA, Ironscales	**Skill up your security: How defenders can harness AI** **Billy McDiarmid,** Sr Director of Sales Engineering, Red Sift	**Strengthening security through simplification: Micro-segmentation with a multi-layered defence** **Richard Meeus,** EMEA Director of Security Technology and Strategy, Akamai & **Brett Ayres,** VP of Product, Teneo	**Securing Microsoft Copilot: Preventing prompt-hacking and data exposure** **William Priestley,** Sales Engineer Manager, Varonis

11:00 Networking break

11:30 **Resourcing priorities in third-party risk management and supply chain security**

Sarah Lawson, CISO & Deputy CIO, University College London; **Clair Phelps,** CISO, Wagestream;
Mark Logsdon, CISO, NHS England; **Gavin Cartwright,** Tech Consulting Lead (TMT), EY

- Identifying, risk assessing and screening critical vendors – a job for who?
- Defining contractual obligation: how do you enforce your security requirements, standards and data handling practices?
- Approaches to continuous vendor monitoring: dealing with problem third parties
- Incident response planning and managing third-party breaches
- What about security vendors?

11:50 **How to create successful malware and defend with Zero Trust**

Seamus Lennon, Vice President of Operations for EMEA, ThreatLocker

- In a world where anyone can create successful malware or have AI generate it for them, it's important to know how malware can be successful so you can better defend
- Starting from a default-deny posture, learn how adopting Zero Trust principles can keep your data safe and operations running regardless of hacking attempts by man or machine

Agenda

12:10 — Addressing today's biggest cybersecurity gap: The human risk factor

Glenn Smith, Principal Sales Engineer, Mimecast

Research shows 8% of employees are responsible for 80% of security incidents. Human risk remains the leading contributor to security breaches, with individuals facing increasingly tailored and frequent attacks. This session will cover:

- How to transform your strategy to address human risk
- Approaches to mitigate human risk in the current threat landscape
- Adopting a human-centric approach to cybersecurity

12:30 — Response and responsibility – this time it's a thriller, not a romantic comedy

James Eason, CRA Practice Lead, Integrity360

- James Eason, Practice Lead for Cyber Risk at Integrity360, tackles the often-overlooked gap between cybersecurity teams and corporate leadership
- He highlights the need for businesses to integrate cyber-risk into boardroom discussions, sharing real-world stories of extortion, insider threats, and governance failures
- With a call to action for CEOs and CISOs to close the communication gap, Eason emphasises that strong cyber-governance isn't just a tech issue – it's key to business survival and reputation, and an under-rated business-enabler

12:50 — Education Seminars | Session 2

Abnormal Security	Cato Networks	Menlo Security	Netwrix	Silverfort	Thales
AI-powered cybersecurity: Combating emerging threats in the era of generative AI **Richard Orange,** Regional Vice President of EMEA, Abnormal Security	**Thinking like a cybercriminal** **Etay Maor,** Chief Security Strategist, Founding Member of Cato CTRL, Cato Networks	**Browser security – the proven prevention layer for enterprise cybersecurity** **Brett Raybould,** Director, Solutions Engineering, Menlo Security	**ITDR that works for you – challenges and how to manage them** **Anthony Moillic,** Field CISO, Netwrix Corporation	**How non-human identities create operational and cyber-risk for organisations** **Peter Batchelor,** UK&I Regional Director, Silverfort & **Al Scott,** Senior Sales Engineer EMEA, Silverfort	**Is data security sexy again – what does the future hold** **Tim Ayling,** VP EMEA Cyber Security Specialists, Thales

13:30 — Lunch networking break

14:30 — Can the AI (R)evolution help security leaders to manage complexity?

Andy Giles, Executive Director, Head of Intelligence Integration, JPMorgan Chase

- Observations of threats using AI for fraud and malware development
- Foundations for effective AI/LLM use, focusing on the importance of a working security data model and appropriate sources
- Potential for AI application in the security risk management context to keep up with the threat
- Importance of training and AI prompt competence
- Personal reflections

14:50 — Security culture eats human risk for breakfast

Noora Ahmed-Moshe, VP of Strategy and Operations, Hoxhunt

- Learn how applying behavioural science and positive psychology fosters a thriving security culture that protects you even against today's AI-driven threats
- Transforming culture and habits requires addressing people's knowledge, behaviour, and attitudes, and that's hard – but measurably doable, at last
- Unravelling the mysteries of human behaviour lets you unlock a level of human risk management well beyond traditional security awareness
- Discover how to foster engagement, turn security from a mandate into a mindset, and transform your employees from your greatest risk into your greatest resource

15:10 — The correlation between dark web exposure and cybersecurity risk

Dave Osler, Head of Product, Searchlight Cyber

- The presentation of a landmark study conducted by the Marsh McLennan Cyber Risk Intelligence Center and Searchlight Cyber
- Research conclusively demonstrating the correlation between an organisation's dark web exposure and cybersecurity risk, based on a sample cyber-insurance loss data from more than nine thousand organisations
- Explanation of different types of dark web exposure and their relative impact on cybersecurity risk both individually and in combination
- Advice on mitigating dark web exposure and cybersecurity risk

15:30 — Networking break

16:00 — Maximising the value of threat intelligence

Parul Khedwal, Security Operations Lead, Trainline; **Evie Wild,** Information Security Officer, EMEA Region, LBBW Bank; **Goher Mohammad,** Group Head of InfoSec, L&Q Group; **Valentina Soria,** Global Head of Cyber Threat Intelligence, UBS

- Paid versus free: where to spend on threat intel
- Data overload or actionable insights? Threat intel and the false positives problem
- The role of AI in extracting the most from threat intel
- Linking enterprise threat intelligence and the business

16:30 — LIVE DEMONSTRATION: Weaponising AI – Voice phishing with AI (Social Engineering 2.0)

Manit Sahib, Ethical Hacker, The Global Fund

- Overview: How AI is being weaponised in the wild for malicious activities
- Use-cases: How to weaponise AI for your own offensive operations
- Weaponising AI for cyber-attacks: AI vishing (AI voice phishing)
- Exploring the new Social Engineering 2.0 technique, AI generated calling Agent (AVA) for vishing. Trained with rejection handling.
- Live demonstration: AI vishing in action. Volunteers? Be ready to come on stage

16:55 — Chairman's closing remarks

17:00 — Drinks reception

18:00 — Conference close

Education Seminars	
Abnormal Security **AI-powered cybersecurity: Combating emerging threats in the era of generative AI** **Richard Orange,** Regional Vice President of EMEA, Abnormal Security	Richard Orange, Regional Vice President of EMEA at Abnormal Security, will explore how the rise of generative AI is transforming both the business and threat landscapes. As AI continues to drive innovation, cybercriminals are using these advancements to launch more sophisticated, high-volume attacks. This session will uncover the real-world threats organisations face today and demonstrate how AI can be leveraged to effectively counter these evolving cyber-risks. Attendees will learn: • The role of generative AI in advancing both innovation and cybersecurity threats • Real-world examples of AI-driven attacks and their impact on organisations • How AI can be harnessed to detect and neutralise sophisticated cyber-threats • Best practices for securing your organisation in a rapidly changing threat landscape
BeyondTrust **Hackers don't hack in – they log in. How to combat the threat of identity compromise** **Lee Elliott,** Director, Solutions Engineering, BeyondTrust	The world of cybersecurity is changing, with more dynamic highly connected systems than ever. With an explosion of apps, accounts and access, the battleground has shifted from traditional perimeter and endpoint security into the world of identity security, effectively meaning the hacker has been replaced by the credentials thief. With identity compromise common to almost every cyber-attack, distinguishing between how a legitimate user is leveraging an identity and the misuse of that identity by an unauthorised user is difficult. This leaves the door open for threat actors to use impersonated identities to access resources, compromise systems, move laterally and achieve their illicit objectives. Today, this is effectively making identity the new security perimeter. Join the discussion with Lee as he shares what is driving this paradigm shift, and how attackers are successfully exploiting the gaps in visibility between IAM and security tools. Attendees will learn: • How the threat landscape is evolving • Real world examples of identity breaches • How attackers are exploiting hidden paths to privilege • How controlling identities and privileges can be your greatest defence
Cato Networks **Thinking like a cybercriminal** **Etay Maor,** Chief Security Strategist, Founding Member of Cato CTRL, Cato Networks	We hear them in many cybersecurity presentations. They are so integrated into marketing campaigns, websites, interviews and product pitches that they have effectively become a universally agreed upon 'truth'. Cybersecurity myths. Not only are they incorrect but they can be downright dangerous. In this session, we will take several of these extremely popular 'truths', explain their origin and how they got to where they are today and then, more importantly, bust these myths using examples from security incidents and recent security research. "Attackers need to be right just once and the defenders need to be right all the time"? "More security products mean better security"? "Sophisticated threat actors use sophisticated tools"? I don't think so… See how threat actors evade security controls, processes, and tools. Attendees will learn: • How threat actors evade security controls • The state of adversarial AI – using, targeting and abusing AI systems • Learn how to implement a multi-chokepoint approach to the attack killchain • Understand how to gain visibility into suspicious network activity • Busting cybersecurity myths

Education Seminars	
Hadrian **How to become proactive and stay ahead of the AI threat curve** **Prash Somaiya,** CTO, Hadrian	Organisations' attack surfaces, IT complexity, and reliance on third parties have increased exponentially, making effective security governance and operations a significant challenge. Meanwhile, the frequency and damage of attacks are increasing, making reactive security strategies no longer economically viable. Attendees will learn: • AI is being used to accelerate the development of exploits leading to faster development • An analysis of vulnerabilities and exploits that challenge the scale and speed of traditional security operations • Security strategies need to transform and focus on proactive and pre-emptive measures • Recommendations for modernising your vulnerability management programme with offensive security.
Ironscales **Go on the offensive by merging AI and human expertise for email security** **Paul Clark,** Head of Sales, EMEA, 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? In this session, we'll explore how to rethink your approach, using AI to combat AI and keep pace with these threats. We'll 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. Attendees will learn: • How email security has evolved in the last decade • How AI is transforming traditional email security approaches • Integrating human insight with AI algorithms • Leveraging AI to create highly accurate and dynamic phishing simulations • The benefits of a holistic approach to secure law firms
Menlo Security **Browser security – the proven prevention layer for enterprise cybersecurity** **Brett Raybould,** Director, Solutions Engineering, Menlo Security	According to Google, 98% of attacks originate from internet usage and 80% of those target end user browsers – sadly all too successfully. Combine this stark reality, with users' relentless demand for new SaaS and private applications, often collaborating with external stakeholders, and security pros are always running to stand still. Attendees will learn: • Security – The proven value of robust browser security across managed and unmanaged devices – automating browser configuration and establishing enhanced browser forensics • Connectivity – Your users and third parties need access to SaaS applications, private web apps and data, including the use of GenAI. We share how organisations are enhancing user protection and productivity while reducing the cost and complexity of solutions such as VDI • Compliance – How browser security supports organisations striving to comply with key NIS 2 requirements for incident management and prevention • We will provide real world examples and case studies of how to increase cyber-prevention through improved browser security
Netwrix **ITDR that works for you – challenges and how to manage them** **Anthony Moillic,** Field CISO, Netwrix Corporation	84% of organisations have suffered identity breaches in the past year. In these attacks, threat actors assume the identity of a legitimate user to compromise systems, move laterally in networks and gain higher levels of access. But these threats are difficult to detect because traditional tools lack the ability to distinguish between a legitimate user and a malicious actor. Therefore, to protect their sensitive data and mission-critical systems, organisations need a comprehensive Identity Threat Detection and Response (ITDR) approach. Attendees will learn: • About the challenges of trying to counter modern attacks and the solutions to help you do so, including Netwrix recent acquisition, PingCastle

Education Seminars	
Red Sift **Skill up your security: How defenders can harness AI** **Billy McDiarmid,** Sr Director of Sales Engineering, Red Sift	• Learn how to enhance LLMs for threat detection and faster security issue resolution • Discover how Red Sift Radar integrates intelligence and automation into workflows • Gain insights on closing security gaps with real-time, actionable data • Explore practical ways to automate security processes with LLMs • See how Radar empowers teams to tackle security issues 10x faster
Silverfort **How non-human identities create operational and cyber-risk for organisations** **Peter Batchelor,** UK&I Regional Director, Silverfort & **Al Scott,** Senior Sales Engineer EMEA, Silverfort	Non-Human Identities (NHIs) pose one of the most significant cyber-threats to an organisation as they can pose severe operational risks. In many cases, NHIs have elevated privileges, lack proper oversight, are not documented, and are often not linked to specific individuals. This makes them attractive targets for attackers, who may exploit them to gain unauthorised access, move laterally within systems, and carry out malicious activities without being detected. In our session, Silverfort will examine how organisations can reduce operational risk by understanding and implementing security controls around their NHIs. Attendees will learn: • Understand why NHIs should be a top priority for your board • Learn about how to measure and detect the level of risk NHIs pose for your organisation • Grow your knowledge of how to mitigate the risk of NHIs, before, during and after a cyber-breach
Teneo & Akamai **Strengthening security through simplification: Micro-segmentation with a multi-layered defence** **Richard Meeus,** EMEA Director of Security Technology and Strategy, Akamai & **Brett Ayres,** VP of Product, Teneo	Attendees will learn: • *Introduction to micro-segmentation:* Understanding how Akamai Guardicore's micro-segmentation technology reduces complexity by isolating and protecting critical assets within the network, minimising attack surfaces • *Integration with multi-layered defence:* Exploring the role of Guardicore Micro-Segmentation in a comprehensive, simplified cyber-defence model, complementing other security layers for enhanced protection • *Simplifying policy management:* Demonstrating how Guardicore's centralised policy management streamlines security operations, reducing administrative burden and minimising the risk of misconfigurations • *Real-world applications:* Case studies showcasing the effectiveness of Guardicore Micro-Segmentation in preventing lateral movement and mitigating the impact of breaches in diverse environments • *Future-proofing cybersecurity:* Discussing the scalability and adaptability of the multi-layered defence model with pro-active micro-segmentation in addressing emerging threats, ensuring long-term security with reduced complexity
Thales **Is data security sexy again – what does the future hold?** **Tim Ayling,** VP EMEA Cyber Security Specialists, Thales	• What is powering the drive for better data security? • Where does this leave current data security? • How do we address these challenges? • How does the future look?
Varonis **Securing Microsoft Copilot: Preventing prompt-hacking and data exposure** **William Priestley,** Sales Engineer Manager, Varonis	Microsoft Copilot has been called one of the most powerful productivity tools on the planet, taking drudgery out of daily work. But Copilot is a different beast than ChatGPT and other AI tools because it has access to everything you've ever worked on in Microsoft 365, and therein lies the hidden risks for information security teams. Attendees will learn: • We'll show you just how easily your company's sensitive data can be exposed using Microsoft Copilot with simple prompts • Our team will then share practical steps and strategies to ensure a secure Microsoft Copilot rollout and prevent prompt-hacking data exposure