Post event report

Strategic Sponsors

Abnormal · TEHEO OPENING MINDS | Akamai · BeyondTrust · GATEWATCHER · Integrity360 your security in mind · mimecast · okta · proofpoint · RANGEFORCE · RED BUTTON DDoS Experts · SEARCHLIGHT CYBER · SentinelOne · TANIUM · tenable · THREATLOCKER

Education Seminar Sponsors

ANOMALI · b!nalyze · CISCO · Commvault · cradlepoint PART OF ERICSSON · infoblox · LOGPOINT · Red Helix · RED SIFT · RISK LEDGER · Silobreaker · SUSE · VARONIS · ZURICH Resilience Solutions

Networking Sponsors

imprivata · iZOOlogic · Metomic

Branding Sponsor

Thomas Murray Risk Intelligence · Due Diligence · Cyber Security

"This was my first e-Crime & Cybersecurity Congress and I was not entirely sure what to expect. The event was very informative with the 'fireside chats' and the 'open forums' of most value to me. Looking forward to the next event!!"

Cyber Security Risk Manager, Thomas Miller

"The e-Crime Congress & Cybersecurity Congress is the one conference I endeavour to attend every year. The agenda is packed yet the sessions are always incredibly well structured – just the right length and the subject matter is always very topical. There's a healthy mix of humour + seriousness when discussing cybersecurity and the inherent risks we're all facing – the speakers know their stuff! One other aspect I really enjoy – there's no hard sell (not like other conferences I've been to)."

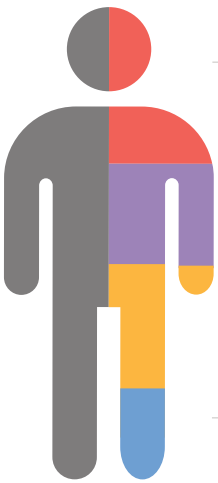
Head of Governance, Risk & Compliance, PwC

Inside this report:

Key themes

- Where's the government when you need it?
- Public-private partnership
- The rise and rise of effective cybersecurity regulation
- Reining in BigTech
- Boosting bang for buck in law enforcement
- Cyber versus crypto
- Developing the next generation of security leaders
- The perimeter is dead – that is not just hype
- From smart machines to smart cities – securing the IoT
- Cloud incident response
- Mapping resources and controls to material business risks
- Embracing risk management

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

Ahmed Aburahal, Technical Product Manager, Integrity360; Dr Kiri Addison, Senior Manager Product Management, Mimecast; Jonathan Armstrong, Partner, Cordery; Ian Ashworth, EMEA Channel Director, Akamai; Brett Ayres, VP of Product, Teneo; Arunava Banerjee, Cyber Risk Consulting Lead, Zurich Resilience Solutions; Simon Brady, Managing Editor & Event Chairman, AKJ Associates; Haydn Brooks, CEO, Risk Ledger; Dhruv Bisani, Head of Adversarial Attack Simulations, Starling Bank; Claire Davies, Partner & CISO, John Lewis Partnership; Andrew Dillon, Sales Engineer, Mimecast; Ian Dutton, Senior Sales Engineer UK, Gatewatcher; Lee Elliott, Director, Solutions Engineering, BeyondTrust; Mike Fell, Director of National Cyber Operations, NHS England; David Ferguson, Deputy CISO, Bank of England; Matt Finn, Information Security Director, DLA Piper; Robert Fitzsimons, Senior Threat Intelligence Engineer, Searchlight Cyber; Rob Flanders, Head of Threat and Incident Response, BAE Systems; Scott Flower, Sr. Solutions Engineering, EMEA, RangeForce; Rich Ford, CTO, Integrity360; Ziv Gadot, CEO, Red Button; Peter Hall, Cloud Security Specialist, Tenable; Christian Have, CTO, Logpoint; Andrew Insley, Cyber Risk Consultant, Zurich Resilience Solutions; Anthon Johnson, Solutions Engineer, Threatlocker; Jain Joseph, Solutions Architect, SUSE; Steve Kinghan, Head of Cyber Operations, Hiscox; David Lomax, Systems Engineering Manager EMEA, APAC, Abnormal Security; Adam Matthews, Senior Solutions Engineer, Okta; Joe Michael, Director and Co-founder, EndpointX; Alistair Mills, Director, Sales Engineering, Northern Europe, Proofpoint; Goher Mohammad, Head of Information Security, L&Q Group; Bernard Montel, EMEA Technical Director and Security Strategist, Tenable; Jorge Montiel, Head of Sales Engineering – EMEA, Red Sift; Sophia N, Head of Incident Response, NCSC; François Normand, Cyber Threat Intelligence Manager, Gatewatcher; Mark Osborne, CISO & Head of Security, GoHenry; Richard Orange, Regional Vice President, EMEA, Abnormal Security; Chris Pace, CMO & Solution Advocate, RangeForce; Gareth Packham, CISO, Save the Children; Ravi Pather, Vice President Sales EME, Ericom Security by Cradlepoint (Ericsson); Dave Philpotts, Sales Engineer, Varonis; Becky Pinkard, Head of Cyber Operations, Barclays; Richard Plumb, Senior Manager Cyber Threat Intelligence, Element Materials Technology; Rob Pocock, Technology Director, Red Helix; Richard Price, CSO, Vorboss;Ben Trethowan, CISO, Brit insurance; Bradley Rossi, Senior Technical Solutions Architect, Cisco; Manit Sahib, Ethical Hacker, The Global Fund; Parthi Sankar, Technical Director N.Europe, Anomali; Jim Simpson, Director of Threat Intelligence, Searchlight Cyber; Mal Smyth, Global Head of Cyber Governance, Risk and Control at Vodafone; Danielle Sudai, Security Operations Manager, Deliveroo; Brett Taylor, SE Director, SentinelOne; Quentyn Taylor, Director of Information Security, Canon (EMEA); Ian Thompson, Head of Cyber-threat Intelligence, BP; Tim Thorne, Product Evangelist, Binalyze Hayley Trezel, Head of CNI Policy, Cyber & Supply Chains, Critical National Infrastructure & Systems Resilience Directorate, Cabinet Office; Lukas Vaivuckas, Intelligence Solutions Consultant, Silobreaker; Oli Venn, SE Manager, Northern Europe, WatchGuard Technologies; Elliott Went, Senior Sales Engineer, UKI, SentinelOne; Samuel Wheeler, Information Security Analyst, Hiscox; Ian Wood, Senior Director Sales Engineering, Commvault; Glyn Worrall, RVP, Technical Account Management, Tanium; Group Captain Robert Wright, DACOS J6 Operations & Cyber, PJHQ

Agenda | Day 1 | 28th February 2024

08:00 Registration and networking break

08:50 Chair's welcome

09:00 **The worst has happened – now what? How to have a 'good' cyber-incident**

Sophia N, Head of Incident Response, NCSC
- A quick primer on incident preparation
- How to minimise harm from an incident after it has happened
- Common mistakes that make an incident more complex and harder to manage
- Balancing short-term and long-term harms in an incident
- How to learn and come back stronger

09:20 **Adapting to the cybersecurity revolution: Unleashing AI for effective defence**

Brett Taylor, SE Director, SentinelOne
- Understand that the digital landscape undergoes seismic transformations and navigating the complexities of the evolving cybersecurity terrain is becoming increasingly difficult
- Explore the indispensable role of artificial intelligence in contemporary defence strategies and why organisations must embrace AI as a linchpin for fortifying their security posture
- Examine why AI has emerged as a critical component in the cybersecurity arsenal. Delve into the limitations of traditional defence mechanisms and underscore how AI, with its ability to learn, adapt, and predict, is essential for keeping pace with the evolving threat landscape
- Delve into AI relevant use cases that give you insights into how you can test the waters of an AI approach, to provide a roadmap for organisations to integrate AI into their cybersecurity strategies effectively

09:40 **Not if, but when – protecting your business against the catastrophic consequences of a cybersecurity breach**

Brett Ayres, VP of Product, Teneo & **Ian Ashworth,** EMEA Channel Director, Akamai
- The evolution of cybercrime, sophisticated attacks, and the role of AI
- Strategies to proactively prepare for a security breach
- Best practices for mitigating the impact of a breach
- Crafting a robust, multi-layered defence strategy

10:00 **FIRESIDE CHAT** **Cyber-risk management: a practitioner's perspective**

Mal Smyth, Global Head of Cyber Governance, Risk and Control at Vodafone
- What's the best way to organise the cybersecurity function in large organisations?
- Are we really managing cyber-risk, or just mapping threats to static frameworks?
- What do you need to change in the face of coming cyber-regulation?
- Security versus resilience: the role of the CISO and the rise of compliance

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

Commvault	**Cyber-resilience for the hybrid world** **Ian Wood,** Senior Director Sales Engineering, Commvault
Logpoint	**Improving threat detection accuracy: Leveraging probability to reduce false positives** **Christian Have,** CTO, Logpoint
Red Button	**Case study: Handling a ransom-driven DDoS attack on a bank** **Ziv Gadot,** CEO, Red Button
Red Sift	**Your path to cyber-resilience** **Jorge Montiel,** Head of Sales Engineering – EMEA, Red Sift
Risk Ledger	**Generative AI and the impact on third-party risk** **Haydn Brooks,** CEO, Risk Ledger
Zurich Resilience Solutions	**Going beyond compliance: Embracing a risk-based approach for enhanced resilience** **Arunava Banerjee,** Cyber Risk Consulting Lead & **Andrew Insley,** Cyber Risk Consultant, Zurich Resilience Solutions

11:00 Networking break

11:30 **Weak links – individual and inventory**

Group Captain Robert Wright, DACOS J6 Operations & Cyber, PJHQ
From experience, poor configuration management and human action are the source of greatest vulnerability. This session will look at the following.
- "It will never happen to me" – Why phishing and other forms of social engineering remain significant threats and some suggestions to improve the situation
- "You can't protect what you can't see" – Why we struggle to understand our IT inventory and are surprised when we fail to protect it
- "The paralysis of uncertainty" – Know your service topography – act at the speed of relevance

11:50 **Team-centric defence: Measuring and maximising your cyber-talent**

Chris Pace, CMO & Solution Advocate, RangeForce
- Challenges of deploying talent to defend your organisation
- The importance of humans to the right of 'boom'
- Technology is only as powerful as the teams who will use it
- Individual training vs Team exercising
- The three Rs of team exercising: Relevance, Realism and Repeatability
- Measuring preparedness aligned to business risk

12:10 **How to defend your workforce with phishing-resistant MFA**

Adam Matthews, Senior Solutions Engineer, Okta
- Traditional multi-factor authentication (MFA) methods are increasingly under attack and are especially prone to phishing
- Discover the three major properties of phishing resistant authenticators
- Understand the best practices for supporting WebAuthn
- Explore the four lines of defence to mitigating phishing attacks
- Learn how to deploy phishing resistant MFA

Agenda | Day 1 | 28th February 2024

12:30 — Protecting against the threat of generative AI

Richard Orange, Regional Vice President, EMEA, Abnormal Security & **Gareth Packham,** CISO, Save the Children

- With rapid advancements in advanced threats, accelerated by the emergence of AI – the emergence of generative models has revolutionised how we work. But the rise of generative AI has also presented challenges for cybersecurity, as malicious actors exploit it to create sophisticated attacks at a higher volume than ever before
- Featuring CISOs from multiple industries, this panel explores how cybercriminals are weaponising email to defraud businesses. Attendees will hear about real-world threats targeting these organisations today and leave understanding there is a new way to fight AI with AI

12:50 — Education Seminars | Session 2

Cisco	**Simplify security** **Bradley Rossi,** Senior Technical Solutions Architect, Cisco
Gatewatcher	**My traffic is encrypted and NDR will see nothing, wanna bet?** **Ian Dutton,** Senior Sales Engineer UK, Gatewatcher
Infoblox	**Uncover sophisticated e-crime attacks with DNS Threat Intelligence** **Trish Almgren,** Senior Product Marketing Manager & Field Evangelist, Infoblox
Red Helix	**What do a tsunami and a cyber-attack have in common?** **Rob Pocock,** Technology Director, Red Helix & **Oli Venn,** SE Manager, Northern Europe, WatchGuard Technologies
Silobreaker	**Beyond bad actors: Building risk-oriented workflows for threat intelligence teams** **Lukas Vaivuckas,** Intelligence Solutions Consultant, Silobreaker
SUSE	**Fortifying Kubernetes: The importance of Zero Trust in Kubernetes environments** **Jain Joseph,** Solutions Architect, SUSE

13:30 Lunch and networking break

14:30 — Third-party security: There must be a better way!

Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator); **Claire Davies,** Partner & CISO, John Lewis Partnership; **Matt Finn,** Information Security Director, DLA Piper; **Goher Mohammad,** Head of Information Security, L&Q Group; **Danielle Sudai,** Security Operations Manager, Deliveroo

- Can we ever really know our supply chain?
- Prioritising information gathering
- Resilience versus security
- Is it time for a complete rethink?

15:00 — Navigating human-centric risk: Unveiling the four elements

Alistair Mills, Director, Sales Engineering, Northern Europe, Proofpoint

- Discover how the human element is both our greatest vulnerability and our most valuable asset in the security equation
- Recognise that individuals play a central role in the success or failure of security measures and that taking a human-centric approach to your security strategy can be pivotal in risk reduction
- Explore the four elements of human-centric risk and set a path to risk reduction with people at the centre of our strategy

15:20 — Protecting against the latest email threats with AI-integrated defences

Dr Kiri Addison, Senior Manager Product Management, Mimecast

Gain insights into the threats of today and how artificial intelligence is being used to protect against them. Attend this session to discover:

- Some of the latest developments in the email threat landscape
- Opportunities for attackers to benefit from recent advances in AI
- How AI can be used as part of an integrated approach to defence

15:40 — Education Seminars | Session 3

BeyondTrust	**Unlocking the key to identity security success: The vital role of PAM** **Lee Elliott,** Director, Solutions Engineering, BeyondTrust
Integrity360	**Securing the modern enterprise: any user, any device, anywhere** **Ahmed Aburahal,** Technical Product Manager, Integrity360
Searchlight Cyber	**How to identify threats to your organisation on the dark web** **Robert Fitzsimons,** Senior Threat Intelligence Engineer, Searchlight Cyber
Tanium	**How do you win at cybersecurity? A strategic approach** **Glyn Worrall,** RVP, Technical Account Management, Tanium
Tenable	**Cloud security and exposure management: Priorities, barriers and risks** **Peter Hall,** Cloud Security Specialist, Tenable

16:20 Networking break

16:40 — EXECUTIVE PANEL DISCUSSION — Prioritising crisis: How to track cyber-threats in a world of competing crises

Richard Plumb, Senior Manager Cyber Threat Intelligence, Element Materials Technology (Moderator); **Rob Flanders,** Head of Threat and Incident Response, BAE Systems; **Ian Thompson,** Head of Cyber-threat Intelligence, BP

- When the world is on fire, where do you install the smoke detectors? Tracking cyber-threat is difficult at the best of times but when everything is a crisis, how do you prioritise?
- Understanding the current threat landscape and what horizon scanning really means in the context of cyber-threat
- How to identify and prioritise the most significant strategic threats and follow those through to operational, tactical, and technical levels
- How to remain adaptable as an organisation to new and emerging threats from multiple vectors
- Where is this all going? What organisations should do now to ensure they are in a better place in 12 months' time

17:10 — LIVE DEMONSTRATION — Weaponising AI for cyber-attacks & offensive operations

Dhruv Bisani, Head of Adversarial Attack Simulations, Starling Bank & **Manit Sahib,** Ethical Hacker, The Global Fund

- Overview & threat landscape: How AI is being leveraged in the wild for malicious activities
- Weaponising AI for offensive operations: Running AI through the cyber-kill chain
- ChatGPT or [insertnamehere]GPT: What's the level of effort required to build your own AI?
- LIVE DEMO: AI in action

17:30 Drinks reception and networking

18:30 Conference close

Agenda | Day 2 | 29th February 2024

08:00 Registration and networking break

08:50 Chair's welcome

09:00 **Annual check-up – taking the pulse of cyber in the NHS**

Mike Fell, Director of National Cyber Operations, NHS England

- The criticality of cyber as a patient safety issue
- Cyber Strategy in Health to 2030
- Lessons we learn from monitoring and defending one of the largest IT ecosystems in the UK

09:20 **The critical foundation for a successful identity security strategy**

Lee Elliott, Director, Solutions Engineering, BeyondTrust

- Introduction to how Privileged Access Management (PAM) is evolving to meet the needs of ITDR
- Understand why identity compromise and misuse are central to almost every cyber-attack and how this is causing a fundamental shift in the cyber-battleground from traditional perimeter and endpoint security into the world of identity security
- Explore why gaps in visibility between Identity Access Management (IAM) and security tools leave the door open for threat actors to use impersonated identities to achieve their illicit objectives
- The progression to a new discipline of Identity Threat Detection and Response (ITDR), which delivers a significant opportunity to secure the identity perimeter

09:40 **Threat intelligence and exposure management; two arms of the same goal – prevention**

Bernard Montel, EMEA Technical Director and Security Strategist, Tenable

- Analyse three recent attack paths
- Question if Cloud security really is so complex
- Are attackers being lazy and using known vulnerabilities? Or are they using brand new techniques?

10:00 **Weaponing your estate – creating an intelligence capability and driving security assurance**

Steve Kinghan, Head of Cyber Operations, Hiscox &
Samuel Wheeler, Information Security Analyst, Hiscox

- Enabling your team and creating space – how and what is required?
- Developing a Purple Team with what & who you have at your disposal
- Aligning capability with the business
- Future considerations – training, retention, remediation…

10:20 **Education Seminars | Session 4**

Anomali	**The expanding role of generative AI in accelerating elite SOC performance** **Parthi Sankar,** Technical Director N.Europe, Anomali
Binalyze	**The growing role of DFIR in resilient incident response strategies** **Tim Thorne,** Product Evangelist, Binalyze
Cradlepoint	**Why are you still experiencing cybersecurity attacks in 2024?** **Ravi Pather,** Vice President Sales EME, Ericom Security by Cradlepoint (Ericsson)
Mimecast	**Work protected: Picking the right battles to avoid over-consolidation** **Andrew Dillon,** Sales Engineer, Mimecast
Proofpoint	**E-pocalypse: Navigating the future of email authentication** **Alistair Mills,** Director, Sales Engineering, Northern Europe, Proofpoint
Varonis	**Is your org ready for Microsoft Copilot?** **Dave Philpotts,** Sales Engineer, Varonis

11:00 Networking break

11:30 **FIRESIDE CHAT** **Mitigating personal liability: The changing climate for security professionals**

Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator);
Quentyn Taylor, Director of Information Security, Canon (EMEA;
Jonathan Armstrong, Partner, Cordery

- The changing politics of security
- Current cases
- Social media scrutiny
- Insurance options for CISOs
- Golden parachutes and legal support

11:50 **Analysis of the Top 3 2023 network attacks, and how an NDR could have avoided them**

François Normand, Cyber Threat Intelligence Manager, Gatewatcher

- Key figures of 2023 threat landscape
- Description and analysis of 3 of the top network attack
- How to anticipate, prevent and detect these threat at the earliest stage

Agenda | Day 2 | 29th February 2024

12:10 From reactive to proactive: Stopping ransomware attacks earlier in the cyber-kill chain

Jim Simpson, Director of Threat Intelligence, Searchlight Cyber

- The most prolific ransomware groups, based on dark web intelligence
- How ransomware groups operate on the dark web
- Spotting Initial Access Brokers selling backdoors into networks on dark web forums
- Identifying and mitigating ransomware attacks earlier in the cyber-kill chain

12:30 Winning at cybersecurity – a strategic approach

Glyn Worrall, RVP, Technical Account Management, Tanium &
Joe Michael, Director and Co-founder, EndpointX

- Review of the technological trends over the last few decades and priorities heading into 2024
- Taking a deeper dive into visibility and control – you cannot protect it if you cannot see it
- Maintaining a good IT hygiene posture through continuous safeguarding
- Do you have the right tools around detection and countermeasures?

12:50 Education Seminars | Session 5

Abnormal Security	**3 new ways cybercriminals are targeting your email** **David Lomax,** Systems Engineering Manager EMEA, APAC, Abnormal Security
Okta	**State of Zero Trust security** **Adam Matthews,** Senior Solutions Engineer, Okta
RangeForce	**Out of the classroom and onto the range: Cybersecurity is a team sport** **Chris Pace,** CMO & Solution Advocate, RangeForce & **Scott Flower,** Sr. Solutions Engineering, EMEA, RangeForce
SentinelOne	**How to eliminate ransomware attacks for good** **Elliott Went,** Senior Sales Engineer, UKI, SentinelOne
Teneo & Akamai	**So, you've been hit by ransomware! What now?** **Brett Ayres,** VP of Product, Teneo & **Ian Ashworth**, EMEA Channel Director, Akamai
ThreatLocker	**Implementing Zero Trust controls on the endpoint** **Anthon Johnson,** Solutions Engineer, Threatlocker

13:30 Lunch and networking break

14:30 Lost in translation

David Ferguson, Deputy CISO, Bank of England

Boards are now pushing back for improved understanding of what they have achieved after years of heavy cyber-investment. As cyber-leaders we're responsible for demonstrating our value to a broad range of stakeholders and to deliver the best ROI with the resources available. So, how do we find the best investments for our organisation and solve the 'lost in translation' problem?

14:50 Red Button: DDoS attacks: Trends and protection strategies

Ziv Gadot, CEO, Red Button

- Why are DDoS attacks so easy to launch today?
- Taking businesses offline - 2023 attack trends and examples
- Gauging your exposure to DDoS threats
- Actionable steps for proactive DDoS protection

15:10 Frontline insights: Ransomware breaches, AI and resilience

Rich Ford, CTO, Integrity360

- Deep dive into the frontline realities of ransomware breaches, drawing from real-world examples by our red team and incident response (IR) team
- Explore how vulnerabilities lead to breaches, highlighting the importance of resilience and proactive exposure management. By dissecting attackers' methods, we underscore the critical role of preparedness and adaptive defence strategies
- Examine the use of Artificial Intelligence (AI) in enhancing detection and prevention efforts, offering a dual perspective on AI's role in both facilitating and combating ransomware attacks
- Gain insights into building more robust defences, leveraging AI for improved security posture, and practical measures for minimising exposure and enhancing organisational resilience against ransomware threats

15:30 Networking break

16:00 Delivering the UK Government Resilience Framework

Hayley Trezel, Head of CNI Policy, Cyber & Supply Chains, Critical National Infrastructure & Systems Resilience Directorate, Cabinet Office

- Do we understand the risks the country faces?
- Is prevention better than cure?
- What does 'whole of society' mean?
- And then there's cyber...

16:20 EXECUTIVE PANEL DISCUSSION The business of being a CISO

Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator);
Mark Osborne, CISO & Head of Security, GoHenry;
Richard Price, CSO, Vorboss;
Ben Trethowan, CISO, Brit insurance;
Becky Pinkard, Head of Cyber Operations, Barclays

- The role of the CISO as security regulation increases (NIS2, DORA etc.)
- Compliance versus security as a true business driver
- The cyber-talent shortage – real or illusion?
- CISO churn: the real causes and effects

16:50 Conference close

Education Seminars	
Abnormal Security **3 new ways cybercriminals are targeting your email** **David Lomax,** Systems Engineering Manager EMEA, APAC, Abnormal Security	New types of impersonation. Better AI. Shifts to collaboration applications. Cybercrime is a business, and criminals are always looking for new ways to steal money. In this session, we will be discussing the latest threat actors and the sift away from the CEO fraud traditionally seen. What attendees will learn: • Why tools like ChatGPT could be dangerous • How you can better protect your organisation from all the latest developments in advanced threats
Anomali **The expanding role of generative AI in accelerating elite SOC performance** **Parthi Sankar,** Technical Director N.Europe, Anomali	Security Operation Centres (SOCs) and those who support them are under relentless pressure to stay ahead of well-funded, unconstrained adversaries that innovate continuously. This dynamic is now being accelerated by the ubiquitous adoption of AI/Generative technologies, which is rapidly taking the global security landscape to an inflection point. What attendees will learn: • This presentation will reassess the CISO mission for the modern digital enterprise against this context • We will discuss the novel application of Natural Language Processing (NLP) and Artificial Intelligence (AI) to Cyber Threat Intelligence (CTI) and SOC operations as it applies to understanding, detecting, operationalising and reporting on external threats against internal telemetry and its role in taking the SOC to elite performance
BeyondTrust **Unlocking the key to identity security success: The vital role of PAM** **Lee Elliott,** Director, Solutions Engineering, BeyondTrust	The world of cybersecurity is changing, with more dynamic highly connected systems than ever. Cloud proliferation has caused an explosion of apps, accounts, and access which makes it now impossible to distinguish between how a legitimate user is leveraging an identity, and how an unauthorised user may be misusing an identity. This has in turn forced the cyber-battleground to shift from traditional perimeter and endpoint security into the world of identity security. Following on from his main agenda session, join Lee as he discusses what is driving this paradigm shift and how attackers are successfully exploiting the gaps in visibility between Identity Access Management (IAM) and security tools, leading to a new discipline of Identity Threat Detection and Response (ITDR). What attendees will learn: • Why identity security is so challenging • How ITDR can provide a centralised view of identities and their entitlements across multi-Cloud and application environments • How ITDR can detect indicators of identity compromise • An example of a real-world identity breach and how it was controlled with ITDR
Binalyze **The growing role of DFIR in resilient incident response strategies** **Tim Thorne,** Product Evangelist, Binalyze	How DFIR is disrupting the traditional digital forensics landscape and delivering forensic capability to the centre of the security stack. What attendees will learn: • Cybersecurity and the growing revolution powered by DFIR • The benefits of speed and automation with DFIR • Leveraging DFIR to reduce caseloads, dwell time, and alert fatigue • Empowerment, resilience, and enhanced security posture thanks to DFIR

Education Seminars	
Cisco **Simplify security** **Bradley Rossi,** Senior Technical Solutions Architect, Cisco	Our attack surface expands rapidly every day in the cloud, datacentre, and our office spaces. But also in areas we don't control thanks to the roaming user. As we try to offer more flexible and agile services to our business and users, we also introduce new threats, vulnerabilities and we have new tools and services to manage. Whilst this is going on, our user experience suffers. What attendees will learn: • The common pain points that we discuss with our customers every day. How do we simplify and solve the user experience problem? As well as how to keep pace with the ever-changing threat landscape fuelled by modern dynamic environments. • Trends and pain points of the industry • User and administrator visibility and experience • Modern solutions that do the heavy lifting
Commvault **Cyber-resilience for the hybrid world** **Ian Wood,** Senior Director Sales Engineering, Commvault	Organisations are facing an increasing number of threats and rising costs due to the hybrid cloud reality year over year. What attendees will learn: • How to simplify modern data protection • How to proactively secure any workload from any location • How to cut costs with authentic cyber-resilience
Cradlepoint **Why are you still experiencing cybersecurity attacks in 2024?** **Ravi Pather,** Vice President Sales EME, Ericom Security by Cradlepoint (Ericsson)	Despite increased spend on security tools, security attacks are still happening. What attendees will learn: • How effective are your security tools in preventing unknown and zero-day attacks? • How do hackers actually breach your security tools? • Should your users be the front line of security defence or is it time to address this differently? • What's THE only way to effectively address unknown and zero-day exploits?
Gatewatcher **My traffic is encrypted and NDR will see nothing, wanna bet?** **Ian Dutton,** Senior Sales Engineer UK, Gatewatcher	Recent times have seen increased encryption of corporate data flows. What attendees will learn: • What are the reasons for this trend? • What can we see on a network today, and what impact does this have on cyber-detection capabilities? • How a Network Detection and Response (NDR) solution can reveal the hidden threats • Demo, case studies and anonymous customer's feedback
Infoblox **Uncover sophisticated e-crime attacks with DNS Threat Intelligence** **Trish Almgren,** Senior Product Marketing Manager & Field Evangelist, Infoblox	In a world where 'Malware-as-a-Service' exists and threats are prolific, pervasive, and persistent, taking a pre-emptive approach to proactively blocking malicious domains can provide a solution. DNS Threat Intelligence is a powerful way to pinpoint and pre-empt malicious cyber-activity, uncovering attacks long before they are declared malicious in the public domain. Attendees will learn how DNS Threat Intelligence can: • Protect your brand by monitoring for lookalike domains • Aggregate threat alerts to deliver actionable insights • Improve the ROI of your existing security stack

Education Seminars	
Integrity360 **Securing the modern enterprise: any user, any device, anywhere** **Ahmed Aburahal,** Technical Product Manager, Integrity360	We will delve into the core principles of Security Service Edge (SSE) and explore its transformative impact on modern enterprises. From the integration of networking and security functionalities to its scalability and flexibility, and why more enterprises are adopting Secure Access Service Edge (SASE) architecture. • Introduction to Security Service Edge (SSE) as a transformative approach in cybersecurity • Exploring how SASE integrates networking and SSE • The benefits and economies of SSE • Real-world examples and practical insights for modern enterprises • Strategic considerations for successful SASE adoption and implementation
Logpoint **Improving threat detection accuracy: Leveraging probability to reduce false positives** **Christian Have,** CTO, Logpoint	This track tackles the challenges of false positives in early-stage attack detection within organisations. Traditional SIEM alerting often leads to a high rate of false positives, posing significant challenges for analysts. What attendees will learn: • Explore how context-driven threat detection, powered by probability scoring, can enhance detection accuracy by consolidating relevant observations into actionable incidents • Context-driven threat detection using algorithms increases detection efficacy by fusing relevant observations to produce high-value incidents • Discuss methods to fuse observations and create high-fidelity alerts, instead of using SIEM to write atomic alerts to detect threats • By alerting on incidents in combination, analysts can detect attacks early in the kill chain while eliminating false positives
Mimecast **Work protected: Picking the right battles to avoid over-consolidation** **Andrew Dillon,** Sales Engineer, Mimecast	Email and collaboration tools are vital to business operations, but they've become arguably the single biggest source of risk to the corporate network. As cloud platforms like Microsoft 365 have grown to dominate business productivity, they've created irresistible targets; and adversaries are using them to deliver everything from phishing to ransomware. What attendees will learn: • How consolidated communications infrastructure offers a rich target for the bad guys • How the technology choices you make can make Microsoft safer and smarter • How you can help your people stay safe and secure by picking the most effective partners for M365
Okta **State of Zero Trust security** **Adam Matthews,** Senior Solutions Engineer, Okta	Okta conducted a global survey to see the progress of the Zero Trust journey for organisations across different industries. This session shares the findings from the study along with ways organisations are keeping their people, assets, and infrastructure safe. What attendees will learn: • Adoption trends and driving factors across different industries and regions • How Zero Trust budgets are shifting due to macroeconomic factors • Challenges organisations are facing in adopting Zero Trust

Education Seminars	
Proofpoint **E-pocalypse: Navigating the future of email authentication** **Alistair Mills,** Director, Sales Engineering, Northern Europe, Proofpoint	In the ever-evolving digital landscape, email authentication has emerged as the unsung hero in safeguarding communication channels. Picture this: What if your customers and business partners suddenly stopped receiving your company's vital emails? Brace yourself for the E-pocalypse, as three major mailbox hosting providers are rolling out stringent email acceptance rules. Join us as we unravel the critical importance of email authentication in today's dynamic cyber-environment. The recent announcements from industry giants have set the stage for a paradigm shift in how emails are validated and accepted. We'll delve into the intricacies of these changes and decipher why it matters now more than ever. What attendees will learn: • *The unseen threats:* Explore the lurking dangers that email authentication aims to thwart, from phishing attacks to unauthorised access • *Decoding the new rules:* Understand the latest email acceptance requirements imposed by leading mailbox providers and how they impact your organisation's communication strategy. • *Strategies for compliance:* Equip yourself with practical insights and strategies to ensure your emails pass the stringent authentication checks, maintaining seamless communication with your audience • *Future-proofing your email strategy:* Gain a foresight into the evolving landscape of email authentication and how your organisation can stay ahead of the curve • Don't be caught off guard! Join us for an insightful journey into the realm of email authentication, and ensure your business is prepared for the challenges and opportunities that lie ahead. The E-pocalypse is near – are you ready?
RangeForce **Out of the classroom and onto the range: Cybersecurity is a team sport** **Chris Pace,** CMO & Solution Advocate, RangeForce & **Scott Flower**, Sr. Solutions Engineering, EMEA, RangeForce	What attendees will learn: • Getting real about recruitment and confidence in talent • The dream of defenders at the top of their game • How to build a culture of continuous improvement • What does realistic and threat relevant team exercising actually look like • A range isn't out of reach, making it work for smaller enterprises
Red Button **Case study: Handling a ransom-driven DDoS attack on a bank** **Ziv Gadot,** CEO, Red Button	What happened when a North American bank received an extortion mail from a hacker group demanding Bitcoin payment and threatening to carry out a DDoS attack? This session will take an insider look at the ways to respond, prepare and mitigate such an attack, based on the experience of Red Button's incident response team. What attendees will learn: • The dynamics of handling and responding to a ransom threat mail • Best practices for incident response procedures • Preparing for a DDoS ransom attack • The role of DDoS simulation tests between attacks

Education Seminars	
Red Helix **What do a tsunami and a cyber-attack have in common?** **Rob Pocock,** Technology Director, Red Helix & **Oli Venn,** SE Manager, Northern Europe, WatchGuard Technologies	How to revolutionise your security through integrated threat detection and rapid response. The need for a unified, comprehensive, and flexible security approach has never been more critical. Just like a tsunami warning system, isolated data points tell you nothing about the coming threat. This presentation explores the paradigm shift from traditional, expensive, and siloed security solutions to comprehensive visibility and threat detection. What attendees will learn: • How embracing Security as a Service can revolutionise cybersecurity for your business, providing a clear path forward to radically transform your security posture • Why traditional security solutions have failed to provide the security assurance your business and board need • Building an integrated mesh architecture through innovative use of established technologies for comprehensive infrastructure monitoring • The benefits of greater visibility across on-premises and cloud environments • How our Threat Monitoring Service can deliver these benefits to you rapidly and reliably through a subscription based SECaaS
Red Sift **Your path to cyber-resilience** **Jorge Montiel,** Head of Sales Engineering – EMEA, Red Sift	Now is the time to delve into strategies for enterprise organisations to uncover, oversee, and safeguard vulnerabilities across their email, domain, and web attack surfaces. The Red Sift Pulse platform has capabilities that can be leveraged. What attendees will learn: • Detect both visible and concealed attacks on their domains proactively • Protect against phishing and BEC attacks • Streamline routine investigations and automate remedial actions • Transition from project-based approaches to continuous processes to effectively combat evolving threats
Risk Ledger **Generative AI and the impact on third-party risk** **Haydn Brooks,** CEO, Risk Ledger	As organisations start to integrate LLMs into business workflows there are added risks to watch out for. What attendees will learn: • What are these added risks? • What are some of the impacts of generative AI specifically on supply chain security? • What risk mitigation strategies are recommended?
Searchlight Cyber **How to identify threats to your organisation on the dark web** **Robert Fitzsimons,** Senior Threat Intelligence Engineer, Searchlight Cyber	Learn how to identify threats on the dark web, based on real-life case studies of organisations that have averted cyber-attacks by monitoring threat actor activity on hidden sites. What attendees will learn: • How to prioritise vulnerability management with dark web intelligence • How to identify Initial Access Broker posts that relate to their network infrastructure • How to monitor ransomware group activity on the dark web

Education Seminars	
SentinelOne **How to eliminate ransomware attacks for good** **Elliott Went,** Senior Sales Engineer, UKI, SentinelOne	Live ransomware can take you from 'business as usual' to a headline breach in a matter of minutes. Join Elliott to engage in an informative session where he will delve into how to eliminate ransomware attacks for good. What attendees will learn: • Insights into how SentinelOne's use of AI – with an emphasis on speed – detects ransomware in milliseconds and prevents similar attacks from becoming breaches. • SentinelOne's patented Rollback feature – where we can take your estate from ransomware breach to pre-breach in a matter of seconds • The latest addition to SentinelOne's platform, a new generative AI interface, PurpleAI, and how it enables analysts to investigate, interpret, and respond to these advanced attacks without any prior experience
Silobreaker **Beyond bad actors: Building risk-oriented workflows for Threat Intelligence Teams** **Lukas Vaivuckas,** Intelligence Solutions Consultant, Silobreaker	CTI teams can take a holistic approach to risk across cyber, geopolitical, reputational, competitor and regulatory threats. What attendees will learn: • Tips on how to action this approach • Integrate threat intelligence into the risk assessment process by identifying relevant PIRs and developing effective responses • Outline the CTI capabilities required to meet the objectives of multiple and varied stakeholders, showcase value, and protect the business from threats
SUSE **Fortifying Kubernetes: The importance of Zero Trust in Kubernetes environments** **Jain Joseph,** Solutions Architect, SUSE	Cloud computing and the shift to container infrastructures accelerate business, yet introduce new security concerns. It is important to ensure you have a security strategy in place and the right tools to help protect against known and unknown attacks. What attendees will learn: • How SUSE helps secure your containerised environment from development to production • Why Zero Trust controls are important in the kubernetes world
Tanium **How do you win at cybersecurity? A strategic approach** **Glyn Worrall,** RVP, Technical Account Management, Tanium	Reviewing the technological trends of the last few decades is an essential part of any strategy. As is setting priorities for 2024. What attendees will learn: • Taking a deeper dive into visibility and control – you cannot protect it if you cannot see it • Maintaining a good IT hygiene posture through continuous safeguarding • Do you have the right tools around detection and Countermeasures?
Tenable **Cloud security and exposure management: Priorities, barriers and risks** **Peter Hall,** Cloud Security Specialist, Tenable	Using research and analyses from multiple sources, this session will discuss how to formulate a strategy to reduce visibility gaps and communicate business risk tied to your exposure. What attendees will learn: • Least privilege access control (everywhere) • Attack surface management • Cyber exposure score

Education Seminars	
Teneo & Akamai **So, you've been hit by ransomware! What now?** **Brett Ayres,** VP of Product, Teneo, & **Ian Ashworth,** EMEA Channel Director, Akamai	Facing a ransomware attack can be a defining moment for any organisation. This education seminar is designed to inform cybersecurity leaders on how to approach a crisis and how to tackle crucial decisions. What attendees will learn: • Should you pay the ransom? • Does the DPA 1998 and Article 32 of the GDPR apply? • Should you tell your customers? • 38% of companies hit with ransomware are hit again within 18 months, how can you be better prepared for next time?
ThreatLocker **Implementing Zero Trust controls on the endpoint** **Anthon Johnson,** Solutions Engineer, Threatlocker	Allowlisting is a central tenet of Zero Trust based security, but rumour has it, it's hard to implement. Join the Threatlocker Team for a demonstration of the controls needed to harden security at the endpoint and simplify operations, from allowlisting and beyond. What attendees will learn: • How to easily implement and manage Application Allowlisting • View the control and visibility organisations gain once implementing Threatlocker • Overview on why organisations implement Zero Trust at the endpoint to deny ransomware by default
Varonis **Is your org ready for Microsoft Copilot?** **Dave Philpotts,** Sales Engineer, Varonis	Microsoft Copilot is now available for enterprise customers, transforming productivity in the Microsoft 365 ecosystem. However, security and privacy concerns have companies hesitant to deploy Copilot. There are operational, regulatory, and reputational risks that every organisation needs to overcome before they can leverage Copilot. If you're going to give people new tools to access and leverage data, you need to make sure that data is secure. The challenge, of course, is that with collaborative, unstructured data platforms like M365, managing permissions is a nightmare that everyone struggles with. What attendees will learn: • How permissions and policies impact Microsoft Copilot security • Important data security posture metrics to measure risk • How to mitigate data security risks before and after deployment • How Varonis and automation can help
Zurich Resilience Solutions **Going beyond compliance: Embracing a risk-based approach for enhanced resilience** **Arunava Banerjee,** Cyber Risk Consulting Lead, Zurich Resilience Solutions & **Andrew Insley,** Cyber Risk Consultant, Zurich Resilience Solutions	There are advantages in adopting a risk over compliance-based approach when building cyber-resilience. What attendees will learn: • How to adopt this resilience and how it brings benefits for you and your organisation • The key principles and strategies for effectively managing cyber-risk as well as enhancing overall resilience • The limitations of a compliance-based approach and its potential gaps in addressing evolving cyber-threats • The risk-based approach model and its role in building a robust cyber-resilience framework • How risk-based decision-making and risk quantification aligns cybersecurity strategies with business objectives to fully optimise budget and resource allocation • Real-life examples where organisations adopting a risk-based approach identified and closed gaps improving their cyber-resilience