Post event report

The 15th e-Crime & Cybersecurity Mid-Year Summit

19th October 2023 | London, UK

Strategic Sponsors

babble

corelight

eSENTIRE

GROUND LABS

okta

SEARCHLIGHT CYBER

SentinelOne

TOKIO MARINE HCC

Education Seminar Sponsors

Abnormal

b!nalyze

Bitdefender

CISCO

cyberhaven

HOXHUNT

Integrity360
your security in mind

JT

KELA

KnowBe4
Human error. Conquered.

mimecast

onetrust

Red Helix

RED SIFT

THALES

THREAT FABRIC

Key themes

Getting real about cyber-risk management

Insuring the uninsurable?

AI for CISOs: the hype versus the reality
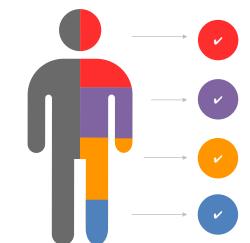
Securing the xIoT

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

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

Ryan Aldred, Head of Cloud Security, **Lloyds Banking Group**

Keith Archer, Commercial Director, **Babble Defence**

Punit Bafna, Information Security Engineering Principal, **BP**

Stephen Bennett, Senior Solutions Engineer, **Okta**

Simon Brady, Event Chairman & Moderator, **AKJ Associates**

Stephen Cavey, Co-founder & Chief Evangelist, **Ground Labs**

Dr. Joseph Da Silva, CISO, **RS Group PLC**

Eleanor Fairford, Deputy Director Incident Management, **National Cyber Security Centre (NCSC)**

Jorge Ferrer Raventos, Principle Solutions Engineering Specialist, **OneTrust**

Zach Fleming, Head of Red Teaming, **Integrity360**

Dave Gill, EMEA Channel Director, **KELA**

Nilesh Halai, SASE Sales Acceleration EMEA, **Cisco**

Mihaela Jembei, Director of Regulatory Cyber, **Information Commissioner's Office (ICO)**

Barry Johnson, Managing Director/CEO at PointWire – Security Engineering Specialists – on behalf of **Corelight**

Christie Jones, Cyber Underwriter, **Tokio Marine HCC**

Matthew Kay, Data Protection Officer, **Metro Bank**

Purvi Kay, Head of Cybersecurity Governance Risk and Compliance, **BAE Systems PLC**

Petri Kuivala, Strategic Advisor, **Hoxhunt**

Andy Lalaguna, Senior Solutions Architect, **eSentire**

Dom Lucas, Head of Security, **British International Investment**

Maurits Lucas, VP of Sales Engineering & Product Marketing, **ThreatFabric**

Javvad Malik, Lead Security Awareness Advocate, **KnowBe4**

Clare Messenger, Commercial Strategy & Business Development Mobile Intelligence, **JT Global**

David Mole, Sales Engineer – EMEA, **Cyberhaven**

Jorge Montiel, Head of Sales Engineering – EMEA, **Red Sift**

Victor Murineanu, Information Security Manager, **Chelsea Football Club**

Malcolm Murphy, Senior Director, Sales Engineering, **Mimecast**

Jason Price, Systems Engineer, **Red Helix**

Marc Pujol, Cyber Security Specialist, **Tokio Marine HCC**

Ketan Pyne, Presales Technical Consultant, **Thales**

Manit Sahib, Ethical Hacker, Contracted to **Global Fund**

Raj Sandhu, Ethical Hacker, Contracted to **World Health Organisation**

Ollie Sheridan, Senior Sales Engineer, **Bitdefender**

Jim Simpson, Director of Threat Intelligence, **Searchlight Cyber**

Tim Thorne, Product Evangelist, **Binalyze**

Elliot Went, Senior Security Engineer, **SentinelOne**

Steven Wills, Senior Systems Engineer, UKIE, **Abnormal Security**

Agenda

08:00	Registration and networking break

09:00 Chairman's welcome and opening remarks

Simon Brady, Managing Editor, AKJ Associates
- Cybersecurity in the spotlight or the headlights?
- A transparency problem: stakeholders want more
- Regulators dial up the pressure: are firms really ready?
- Plus ça change…….

09:20 Why Cloud should make us think differently about security

Ryan Aldred, Head of Cloud Security, Lloyds Banking Group
- Firstly, is Cloud secure?
- The realities of a shared responsibility model
- Continuous deployment, failing fast & agile. How does security keep up?
- Do we understand our new perimeter? What perimeter?
- Infrastructure-as-Code, Security-as-Code, Everything-as-Code!
- Are you ready?

09:40 From prey to play: Think like an attacker to level up your security

Elliot Went, Senior Security Engineer, SentinelOne
Join Senior Security Engineer, Elliot Went as he delves into:
- An overview of the current threat landscape: Current trends and how to mitigate
- Sentinel Labs: The engine behind SentinelOne's threat intelligence and how their research fuels technology
- Real world threat hunting case studies
- How to take S1 for a test drive – threat hunting workshops

10:00 The misperceptions of the cybersecurity skills gap

Purvi Kay, Head of Cybersecurity Governance Risk and Compliance, BAE Systems PLC
- The fast-paced growth of digitalisation and rising demand for cyber-professionals only increases the cyber-skills gap
- Or have we created an 'artificial skills gap' due to some misperceptions?
- This talk focuses on addressing some of these misperceptions that will help widen the cyber-talent pool and improve the recruitment and retention of skilled professionals

10:20 Education Seminars | Session 1

Abnormal Security	Bitdefender	Cisco	KnowBe4	Thales	ThreatFabric
3 new ways cybercriminals are targeting your email	**How do you know what to look for when threat hunting?**	**Frustrate attackers, not users – secure, exceptional user experience**	**2023 Phishing By Industry Benchmarking report: how does your organisation measure up**	**A day in the life of 'YOUR' sensitive data**	**Your phone: The new frontier of malware, scams and fraud**
Steven Wills, Senior Systems Engineer, UKIE, Abnormal Security	**Ollie Sheridan,** Senior Sales Engineer, Bitdefender	**Nilesh Halai,** SASE Sales Acceleration EMEA, Cisco	**Javvad Malik,** Lead Security Awareness Advocate, KnowBe4	**Ketan Pyne,** Presales Technical Consultant, Thales	**Maurits Lucas,** VP of Sales Engineering & Product Marketing, ThreatFabric

11:00	Networking break

11:30 The Importance of transparency

Eleanor Fairford, Deputy Director Incident Management, National Cyber Security Centre (NCSC);
Mihaela Jembei, Director of Regulatory Cyber, Information Commissioner's Office (ICO)
- Why it's in everyone's interests to be more open about cyber-attacks
- Exploring and dispelling the myths around responding to cyber-attacks
- How cybercriminals prey on misconception
- Your regulatory responsibilities and beyond
- What we do and how we can help

11:50 Cyber-breach walkthrough: How to build cyber-resilience to prevent disruption

Andy Lalaguna, Senior Solutions Architect, eSentire & **Keith Archer,** Commercial Director, Babble Defence
An interactive cybersecurity breach presentation covering:
- The most disruptive emerging cyber-threats currently being tracked by eSentire
- How you can build cyber-resilience to prevent business disruption
- How eSentire and Babble work together to deliver cyber-resilience in real-world use cases

Agenda

12:10 — **The top ways threat actors target organisations from the dark web**

Jim Simpson, Director of Threat Intelligence, Searchlight Cyber
- The top cybercriminal activity that can be observed on the dark web, including: initial access brokers, insider threats, and supply chain reconnaissance
- How organisations monitoring the dark web can identify this activity and enhance their defences
- Case study examples of how early warning on the dark web has been used to identify and stop cyber-attacks in their tracks

12:30 — **Cyber-threats and risk transfer through insurance**

Christie Jones, Cyber Underwriter & **Marc Pujol,** Cyber Security Specialist, Tokio Marine HCC
- Key trends in cyber-risk
- Cyber-risk analysis across sectors and jurisdictions
- Risk management solutions offered by insurance

12:50 — **Education Seminars | Session 2**

Ground Labs	Hoxhunt	Integrity360	Mimecast	OneTrust	Red Sift
Data awareness: A three-step model to mitigate data theft **Stephen Cavey,** Co-founder & Chief Evangelist, Ground Labs	**The future of the human risk reduction** **Petri Kuivala,** Strategic Advisor, Hoxhunt	**Evolution of attackers & the need for red teaming in modern cybersecurity** **Zach Fleming,** Head of Red Teaming, Integrity360	**Thwarting the Barbarians: Gates, guards & governance** **Malcolm Murphy,** Senior Director, Sales Engineering, Mimecast	**Breaking down Europe's top InfoSec & cybersecurity frameworks: Tips to evaluate your current state or next steps** **Jorge Ferrer Raventos,** Principle Solutions Engineering Specialist, OneTrust	**Your path to cyber-resilience** **Jorge Montiel,** Head of Sales Engineering – EMEA, Red Sift

13:30 — Lunch and networking break

14:30 — **Getting ahead of generative AI risk**

Dr. Joseph Da Silva, CISO, RS Group PLC
- Why generative AI isn't going away
- How emerging AI regulation is going to impact all businesses
- How we (a FTSE100 company) are currently approaching the risk/benefit case
- What we are saying to our employees

14:50 — **How to defend your workforce with phishing-resistant MFA**

Stephen Bennett, Senior Solutions Engineer, Okta
- Even with a high cost of failure, why do organisations continue to fall for credential-based phishing attacks?
- Is it time to reevaluate the reliability of traditional MFA methods?
- Find out how leading companies are leveraging advanced, secure alternatives to deliver phishing-resistant authentication

15:10 — **You forgot you left the network on...**

Barry Johnson, Managing Director/CEO at PointWire – Security Engineering Specialists – on behalf of Corelight
- Cyber-defence spend focuses a lot on perimeter and endpoint protection, but what about the traffic which does get through?
- Lateral movement occurs by moving East > West on your network because your traditional defences already failed
- Come and learn about how Corelight can help provide network visibility to cover IoT, OT, managed & unmanaged endpoint traffic visibility

15:30 — **Education Seminars | Session 3**

Binalyze	Cyberhaven	JT Global	KELA	Red Helix
The growing role of DFIR in resilient incident response strategies **Tim Thorne,** Product Evangelist, Binalyze	**What is data lineage? (And how it's transforming data security)** **David Mole,** Sales Engineer – EMEA, Cyberhaven	**Bringing mobile intelligence to the fight against fraud** **Clare Messenger,** Commercial Strategy & Business Development Mobile Intelligence, JT Global	**Exploring the cybercrime ecosystem** **Dave Gill,** EMEA Channel Director, KELA	**How to build a resilient human firewall** **Jason Price,** Systems Engineer, Red Helix & **Javvad Malik,** Lead Security Awareness Advocate, Knowbe4

16:10 — Networking break

16:30 — **EXECUTIVE PANEL DISCUSSION** — **Senior leadership**

Simon Brady, Event Chairman & Moderator, AKJ Associates; **Punit Bafna,** Information Security Engineering Principal, BP; **Dom Lucas,** Head of Security, British International Investment; **Victor Murineanu,** Information Security Manager, Chelsea Football Club; **Stephen Cavey,** Co-founder & Chief Evangelist, Ground Labs; **Matthew Kay,** Data Protection Officer, Metro Bank
- Integrating cybersecurity into wider enterprise risk management frameworks
- Becoming a more strategic partner to the business?
- Building resilience against third-party security threats
- Web 3.0 and the next generation of the internet: securing new technologies and service

17:10 — **Bypassing multi-factor authentication (MFA) via phishing techniques**

Manit Sahib, Ethical Hacker, Contracted to Global Fund & **Raj Sandhu,** Ethical Hacker, Contracted to World Health Organisation
- Introduction to MFA bypass phishing techniques
- Live demonstration of MFA bypass attack
- Countermeasures and best practices
- Conclusion of demo and presentation

17:30 Chairman's closing remarks	**17:35** Drinks reception and networking break	**18:30** Conference close

Education Seminars

Abnormal Security

3 new ways cybercriminals are targeting your email

Steven Wills, Senior Systems Engineer, UKIE, 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.

Join us for this session where Steven Wills, Senior Systems Engineer, UKIE, will discuss:

- How threat actors are shifting away from the CEO fraud of the past
- Why tools like ChatGPT could be incredibly dangerous
- What new threats are on the horizon
- And how you can better protect your organisation from all of it

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.

Key takeaways:

- 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

Bitdefender

How do you know what to look for when threat hunting?

Ollie Sheridan, Senior Sales Engineer, Bitdefender

With an increasingly large amount of data being logged in to SIEMs, a treasure trove of data avails itself for both current and retrospective analysis. When approaching this huge amount of data, where do you start? Having access to known threats and possible indications of compromise, you can equip yourself you with the tools needed to hunt down and eliminate known threats within our environment, resulting in more secure systems.

- How to automate threat hunting within the data you have collated
- How Bitdefender makes this high-fidelity data available
- Understand the extent of C2C DNS requests, malicious IP connectivity and the existence of unwanted files within your environment
- Learn how this can improve your security posture and accelerate investigations by your SOC team

Cisco

Frustrate attackers, not users – secure, exceptional user experience

Nilesh Halai, SASE Sales Acceleration EMEA, Cisco

Today's digital landscape is constantly changing, and modern networks extend from the private datacentre to the cloud to the remote user, including their professional and personal devices. This complexity has led to larger attack surfaces, resulting in more threats and in response, more intrusive security measures.

Traditionally, stronger security created more complex management, forcing administrators to manage an average of 76 different security tools, and this complexity can allow attackers to persist on the network longer without detection. It also creates a poorer end user experience, requiring users to login repeatedly and manage their VPN connection, which frustrates users and sometimes leads them to circumvent security practices.

In this presentation, we will cover the prevailing industry trends, pain points, and look at the roles of modern solutions like Secure Service Edge (SSE) and Extended Detection and Response (XDR) in countering and alleviating these pain points.

- Trends and pain points
- User experience versus security
- Admin experience and visibility
- Modern solutions (SSE and XDR)

Education Seminars	
Cyberhaven **What is data lineage? (And how it's transforming data security)** **David Mole,** Sales Engineer-EMEA, Cyberhaven	For over 20 years, data security technology has relied on content analysis to automatically classify data. Whether you're using simple RegEx or complex machine learning, there are limits to what kinds of data you can classify by looking at the content alone. Enter, data lineage. Advances in graph database technology have made it possible to track all data within an organisation – where it originated, where it went, and who modified it. Whether client documents, source code, or product designs, data lineage is making it possible to protect a wider range of sensitive information with fewer false positives than ever before. This session will cover an overview of data lineage and how it's changing security with: • Visibility into how data moves within your organisation • Better data classification than content-based approaches • Rich context to accelerate investigations
Ground Labs **Data awareness: A three-step model to mitigate data theft** **Stephen Cavey,** Co-founder & Chief Evangelist, Ground Labs	Data theft continues to grow in both frequency and scale. There's never been a better time for organisations to establish an evidence-based approach to data awareness for data security. In this session, you'll learn: • How your company may be inadvertently enabling data theft and subsequent identity fraud through its data practices • Why data awareness is crucial to effectively identifying and managing your risk of data theft • How adopting a three-step model to enhance your data awareness with evidence-based discovery helps mitigate your risk of data theft amid emerging threats and increasing data regulation
Hoxhunt **The future of the human risk reduction** **Petri Kuivala,** Strategic Advisor, Hoxhunt	Cybersecurity comes together in a holy marriage of people, processes and technology. CISOs need to engage people as their force multipliers as they will not survive alone in the constantly evolving world. Join this interactive session to learn more about: • The CISO veteran & start-up coach's thoughts about the people role in future with the cybersecurity context • Be ready with your phone having www.menti.com open to donate your ideas back into the conversation. "Hold on to your chair as Texas is going bye bye….the Matrix".
Integrity360 **Evolution of attackers & the need for red teaming in modern cybersecurity** **Zach Fleming,** Head of Red Teaming, Integrity360	Join Integrity360's Head of Red Teaming, Zach Fleming, for a deep dive into the constantly changing threat landscape and gain insights into how attackers have evolved, bypassing even the latest and most sophisticated tooling. Going beyond the tools and technology, Zach will also shed light on the often-overlooked element of human error. Learn how regular red teaming exercises can be the critical difference in ensuring robust cybersecurity in today's dynamic environment. In this session: • *The modern attacker:* An insight into how cyber-adversaries have evolved over the years, now leveraging sophisticated tools to outsmart conventional defence mechanisms • *Beyond technology:* How the human element, often neglected in cybersecurity discourse, can become the weakest link, rendering state-of-the-art tools ineffective • *Workload pressures:* Understand how the stresses of increasing workloads can diminish the efficacy of security solutions, making organisations more vulnerable to breaches • *Red teaming – not just a luxury:* Recognise that red teaming is no longer an optional exercise for large corporations but a necessity for businesses of all sizes in ensuring a resilient defence against evolving threats • *Marrying tech & talent:* The realisation that even the best technologies are only as good as the professionals behind them, emphasising the importance of capacity and capability in tandem

Education Seminars

JT Global

Bringing mobile intelligence to the fight against fraud

Clare Messenger, Commercial Strategy & Business Development Mobile Intelligence, JT Global

With fraud an ever present and rapidly evolving threat to individuals and businesses we look at how mobile intelligence data can be used to detect and prevent fraud, create better secure authentication experiences for customers, and add real-time value to KYC checks.

To successfully fight fraud demands an intimate understanding of how it's perpetrated and how technology and social trends are driving it. Without the understanding of how cybercriminals are exploiting opportunities, organisations often fail to create robust and holistic fraud prevention measures that can detect and prevent fraud from happening in the first instance.

Mobile network operators hold a vast amount of real-time data that can be interrogated and leveraged to combat today's most common and harmful frauds such as SIM swap fraud, account takeover and authorised push payment fraud. Exposing the right data at the right time can and is having positive results for financial services battling a torrent of multiple attack vectors.

- Educating organisations about the threats from fraud
- The wealth of data from MNOs
- Creating better customer experiences
- How greater collaboration will fight the war on fraud

KELA

Exploring the cybercrime ecosystem

Dave Gill, EMEA Channel Director, KELA

- Understand and simplify the complex world of the cybercrime ecosystem
- Gain insights into the motivations, tactics, and strategies of cybercriminals
- Learn how defenders can protect their organisation's assets

KnowBe4

2023 Phishing By Industry Benchmarking Report: How does your organisation measure up

Javvad Malik, Lead Security Awareness Advocate, KnowBe4

As a security leader, you have a lot on your plate. Even as you increase your budget for sophisticated security software, your exposure to cybercrime keeps going up. IT security seems to be a race between effective technology and ever-evolving attack strategies from the threat actors. However, there's an often-overlooked security layer that can significantly reduce your organisation's attack surface: New-school security awareness training.

- Understanding who's at risk and what you can do about it
- Actionable tips to create your 'human firewall'
- The value of new-school security awareness training

Mimecast

Thwarting the Barbarians: Gates, guards and governance

Malcolm Murphy, Senior Director, Sales Engineering, Mimecast
Let's put the noise to one side

for a moment. Most attacks start with an email, and that gives us great insight into what attacks are actually out there right now. Once we know that, we can determine how best to respond: what we need from technology and how to enable our people to play their part.

What you will learn:

- The nature of today's threat landscape
- The role users play in maintaining security
- Where AI is useful, and why over-reliance is risky
- How to get the most out of your cyber-security investments

OneTrust

Breaking down Europe's top InfoSec & cybersecurity frameworks: Tips to evaluate your current state or next steps

Jorge Ferrer Raventos, Principle Solutions Engineering Specialist, OneTrust

Join us as we break down the ins and outs of ISO/IEC 27001 in comparison to SOC 2, the EU Cybersecurity Act, the NIS2 Directive, the Digital Operational Resilience Act (DORA) or the UK Cyber Essentials as other examples of standards to keep top of mind.

- Review the timelines, frequency, and scope of the latest updates across Europe's most referenced frameworks
- Understand what frameworks might be the best fit for your organisation based on business needs and resources
- Identify framework overlap and programme considerations to remove duplication, complexity, and effectively test once, comply many

Education Seminars

Red Helix

How to build a resilient human firewall

Jason Price, Systems Engineer, Red Helix & **Javvad Malik,** Lead Security Awareness Advocate, Knowbe4

Most cyber-attacks begin with phishing and so your 'human firewall' can be either your strongest or weakest defence. But building a resilient human firewall involves changing behaviour, which is always a challenge.

In this presentation, we will equip you with the theory and real-world examples to:

- Grow a positive culture of personal responsibility for cyber-hygiene
- Teach your staff to spot clever phishing and spoofing emails for what they are
- Empower people to signal when they think they've been scammed

We will provide practical examples of how we improve cyber-vigilance for our clients so that you leave the session equipped with sure fire strategies to strengthen the security culture in your organisation.

Red Sift

Your path to cyber-resilience

Jorge Montiel, Head of Sales Engineering – EMEA, Red Sift

In this session, Jorge Montiel will explore how enterprise organisations can discover, manage and protect vulnerabilities across their email, domain, and web attack surfaces.

Drawing on the capabilities of Red Sift's Digital Resilience Platform, he will cover how organisations can:

- Detect seen and unseen attacks on your domain before they do any damage
- Simplify routine investigation and automate remediation
- Go from projects to process – attacks don't work on a quarterly basis, so you can't afford to either

Thales

A day in the life of 'YOUR' sensitive data

Ketan Pyne, Presales Technical Consultant, Thales\

Today's businesses and governments depend on the cloud, data, and software to deliver trusted digital services. That is why the most recognised brands and organisations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centres to devices and across networks. As the global leader in data security and software licensing, Thales solutions enables organisations to move to the cloud securely, achieve compliance with confidence, create more value from their software, and deliver seamless digital experiences for millions of consumers every day.

Whether you're looking to guard against abuse by privileged users, encrypt sensitive data in a database, or address your compliance mandates in the cloud, Thales can help.

Key takeaways:

- What do you know about the data that you are unknowingly generating and disclosing?
- What are the responsibilities of the 3rd parties who acquire your data?
- Can you do anything about it?
- Learn good basic cybersecurity practices by managing your daily information disclosure and consumption

ThreatFabric

Your phone: The new frontier of malware, scams and fraud

Maurits Lucas, VP of Sales Engineering & Product Marketing, ThreatFabric

ThreatFabric has built their reputation by discovering over 80% of all mobile malware families. As the frontier of cyber-threats is increasingly shifting to mobile devices, we invite you to join us to learn about the latest updates on the mobile threat landscape, along with emerging trends and threats in the UK (and neighbouring countries). You'll learn how the frontier is moving; and we'll answer the most important questions: has it moved to the UK and what does this mean for your organisation and customers?

What you'll learn:

- The UK mobile threat landscape
- Latest methods of how victims are compromised
- Trends in Device TakeOver (DTO), droppers and distribution, most popular malware families and how they are operated
- What you can do to be proactive