Post event report

e-crime & cybersecurity CONGRESS

The 21st e-Crime & Cybersecurity Congress

1st & 2nd March 2023 | London, UK

Strategic Sponsors

Abnormal
BeyondTrust
corelight
CROWDSTRIKE
Forcepoint
GATEWATCHER
Integrity360 your security in mind
MENLO SECURITY
mimecast
proofpoint.
RED SIFT
SentinelOne
SYNOPSYS
transmit security

Education Seminar Sponsors

cisco
eSENTIRE
HOXHUNT
INTEL471
Kiteworks
noetic
OBSIDIAN
Ontinue
opensystems
RISK LEDGER
SEARCHLIGHT CYBER
Silobreaker
VMRAY
ZEROFOX

Networking Sponsors

iZOOlogic
PERCEPTION POINT
ULTRARED Validated cyber intelligence

Branding Sponsors

agnostic intelligence
BSS.
JT

> “I thought the e-Crime & Cybersecurity Congress was absolutely fascinating! I'm new to the industry, so there was a lot for me to learn in a short time. Many of the topics discussed were advanced, but the speakers were excellent at explaining things and I was able to understand every point. The whole thing was so incredibly well organised and well run and I'm really looking forward to going back next year!”

**Software Engineer,
The Home Office**

> “Happy 21st! – great to be back in person at another well organised event providing short, punchy and educational presentations from some quality speakers.”

**Chief Compliance and Business Ethics Officer,
Saint-Gobain**

> “Just wanted to let you know I thought it was a really good event!”

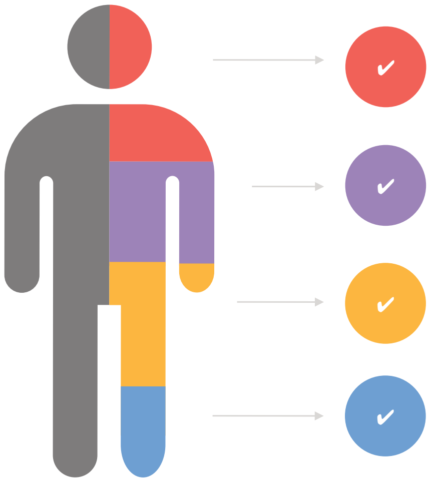
**Information Security Programme Manager,
Hiscox**

Inside this report:

Key themes

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

Who attended?



Cyber-security

We have a 15-year track record of producing the events cyber-security professionals take seriously

Risk Management

We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance

We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy

We are a key venue for decision-makers with budget and purchasing authority

Speakers

Michael Bourton, Senior Security Solutions Engineer EMEA & APAC, VMRay; Matthew Brady, Sales Engineering Manager, Synopsys; Haydn Brooks, CEO, Risk Ledger; James Burchell, Senior Security Engineer, CrowdStrike; Lt Col Chris Cameron, Head of Cybersecurity, Permanent Joint Headquarters, UK Strategic Command; Scott Chenery, Regional Manager, Kiteworks; Richard Combes, Senior Manager – Technical Sales, Proofpoint; Jane Corr, CISO, Canada Life Group Services Europe; Joseph Da Silva, CISO, RS Group; Darcy Delich-Coull, CISO, Footasylum; Johan Dreyer, Field Chief Technology Officer, Mimecast; Ian Dutton, Senior Sales Engineer, Gatewatcher; Richard Ford, Chief Technology Officer, Integrity360; Simon Goldsmith, Head of Information Security, OVO Energy; Andrew Gould, Detective Chief Superintendent, National Cybercrime Programme Lead; Irfan Hemani, Deputy Director of Cybersecurity and Digital Identity, Department for Science, Innovation and Technology; Sam Hooke, Hoxhunt; Ash Hunt, CISO, Apex Group; Ben Johnson, CTO and Co-founder, Obsidian Security; Adrian Jones, Country Manager UK & Ireland, Gatewatcher; Khalid Khan, Cybersecurity Strategist, Forcepoint; Andy Lalaguna, Senior Solutions Architect, eSentire; Sarah Lawson, CISO, UCL; Rob Lay, Leader, Systems Engineering, Cisco; Jonathan Lee, Sr. Product Manager, Menlo Security; Mark Logsdon, CISO, NHS Digital; Dave Lomax, SE Director, EMEA, Abnormal Security; Maurits Lucas, Director of Product Marketing, Intel 471; Eleanor Ludlam, Partner, DAC BEACHCROFT; Maurice Luizink, Director, Solutions Engineering, Transmit Security; David Mahdi, Chief Strategy Officer, Transmit Security; Chris Martin, Senior Director, EMEA, Abnormal Security; James Maude, Lead Cybersecurity Researcher, BeyondTrust; Adam Maxwell, Head of Information Security, Doctor Care Anywhere; Tom McVey, Solution Architect, Menlo Security; Jesús Mérida Sanabria, CISO, Iberia; Alistair Mills, Director, Sales Engineering, Proofpoint; Jorge Montiel, Head of Sales Engineering – EMEA, Red Sift; Aaron Mulgrew, Solutions Architect, Forcepoint; Chris Neely, Director of Sales Engineering, Noetic Cyber; Simon Newman, CEO, The Cyber Resilience Centre for London; François Normand, Cyber Threat Intelligence Manager, Gatewatcher; PJ Norris, Senior Security Engineer, SentinelOne; Ashley 'AJ' Nurcombe, Senior Cybersecurity Consultant – UK&I, Corelight; Gareth Owenson, Chief Technology Officer and Co-founder, Searchlight; Keir P, Head of Strategic Response, National Cybersecurity Centre (NCSC); Jensen Penalosa, Assistant Legal Attaché, FBI; Drew Perry, Chief Innovation Officer, Ontinue; Stuart Peters, Head Cyber Resilience Policy Cybersecurity and Digital Identity Directorate, Department for Science, Innovation and Technology; Becky Pinkard, Head of Cyber Operations, Barclays; Helen Rabe, CISO, BBC; Ben Readings, Field Solutions Engineer, Kiteworks; Grant Revan, Head of Strategic Engagement, Red Sift; Lewis Shields, Principal Intelligence Analyst, ZeroFox; Martyn Styles, Head of Information Security, Bird & Bird LLP; Kevin Tongs, Account Executive, Silobreaker; Jon Townsend, CIO, National Trust; Andrea Walker, Head of Information Security, BBC; Michael White, Principal Architect, Synopsys

Agenda | Day 1 | 1st March 2023

08:00 Registration and networking break

08:50 Chairman's welcome

09:00 **None of us is as smart as all of us**

Keir P, Head of Strategic Response, National Cybersecurity Centre (NCSC)

- Changes to the cyber-threat
- Changes to the cyber-ecosystem
- How can you respond?
- How can we work together?

09:20 **Puzzling through the XDR jigsaw pieces: Buzzword or genuine security movement?**

PJ Norris, Senior Security Engineer, SentinelOne

Join PJ Norris, Senior Security Engineer, at SentinelOne, as he helps us look beyond the acronyms, explains the history and development of XDR practice, and decodes the secrets of enrolling a successful XDR technology across your network.

- XDR. It's the hottest domain in the cyber-world right now and the biggest buzzword you'll see plastered over LinkedIn and debated amongst security vendors
- But ask around and you'll find very few people truly understand the field and even fewer know what the initials stand for
- Is it just a marketing buzz, or is there a profound and significant movement occurring?

09:40 **Cybersecurity physics: Breaking the attack chain**

James Maude, Lead Cybersecurity Researcher, BeyondTrust

Join BeyondTrust and learn how you can break the attack chain and establish a solid foundation for security project success. James Maude, Lead Cybersecurity Researcher, will cover:

- Common attack chain entry points
- Practical steps you can take to block entry
- How PAM ensures project success

10:00 **The evolving scale of disinformation**

Helen Rabe, CISO, BBC, and **Andrea Walker,** Head of Information Security, BBC

- The effects on the security profession and potential regulatory implications
- Career opportunities as a specialism
- Where does this sit? DPO management sphere or InfoSec?

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

Abnormal Security	**More attacks, more problems: 7 key elements of effective email security** **Dave Lomax,** SE Director, EMEA, Abnormal Security
Cisco	**Why productivity and security need to be two sides of the same coin** **Rob Lay,** Leader, Systems Engineering, Cisco
Menlo Security	**The next class of browser-based attacks** **Tom McVey,** Solution Architect, Menlo Security
Proofpoint	**Rethink your approach to data loss prevention** **Richard Combes,** Senior Manager – Technical Sales, Proofpoint
Red Sift	**Protect your digital brand in 2023** **Jorge Montiel,** Head of Sales Engineering – EMEA, Red Sift
Synopsys	**From SCA, to software supply chain risk management to SBOM** **Matthew Brady,** Sales Engineering Manager, Synopsys

11:00 Networking break

11:30 **War in the fifth domain: The implications of the Russian invasion of Ukraine**

Lt Col Chris Cameron, Head of Cybersecurity, Permanent Joint Headquarters, UK Strategic Command

- The threat landscape in cyberspace
- The confusion between nation-state hackers and hacktivist groups – and their overlap
- What we (PJHQ) did in response to the war
- Why did the big Russian cyber-attack never manifest itself?

11:50 **Is it time to panic? How attackers are leveraging ChatGPT – And how AI can help mitigate their attacks**

David Mahdi, Chief Strategy Officer, Transmit Security

- A few months after its release, attackers are already exploring ways to leverage ChatGPT's ability to generate custom code and humanlike writing in response to prompts
- Security researchers are anticipating that ChatGPT will only add to the volume and velocity of attacks, both new and repurposed
- But cybersecurity leaders shouldn't panic: ChatGPT and other AI tools can also benefit cybersecurity teams
- How do we make sense of all of this? Is it truly good or bad? In this keynote, we cover this hot topic and what cybersecurity leaders should know about it

12:10 **Is network evidence really needed for security operations?**

Ashley 'AJ' Nurcombe, Senior Cybersecurity Consultant – UK&I, Corelight

- Do you consider network evidence a crucial part of your SOC strategy?
- How do you really know which alerts are the most serious?
- What's the best way to shift from responding to alerts to hunting for threats?
- Understand how to stay ahead of ever-changing attacks by using a data-first approach for detection and response

12:30 **New year, new attacks: 3 ways cybercriminals target you**

Chris Martin, Senior Director, EMEA, Abnormal Security

- More advanced security tools do not always give advanced protection – not when attackers change their tactics
- Why is it email attacks today are so different from what we saw a decade – or even a year ago?
- Did you know that the sophistication of attacks means that only 2.1% will be reported to your SOC Team?
- Want to see an overview on threat actors use email and social engineering to run their scams?
- Learn what you can do to stop these attacks before they land in employees' inboxes and see some real world examples of these attacks

Agenda | Day 1 | 1st March 2023

12:50	**Education Seminars | Session 2**	
	CrowdStrike	**The external attack surface is constantly changing. How can you identify unknown risks and exposures in real time?** **James Burchell,** Senior Security Engineer, CrowdStrike
	Intel 471	**The seven habits of effective cybercriminals** **Maurits Lucas,** Director of Product Marketing, Intel 471
	Ontinue	**SecOps automation in Microsoft Teams?** **Drew Perry,** Chief Innovation Officer, Ontinue
	Silobreaker	**Tools and tactics to solve the top 3 Open-Source Intelligence (OSINT) challenges** **Kevin Tongs,** Account Executive, Silobreaker
	VMRay	**Getting sand in funny places: Understanding malware sandboxing** **Michael Bourton,** Senior Security Solutions Engineer EMEA & APAC, VMRay
13:30	Lunch and networking break	
14:30	**One CISO's guide to embracing risk management**	
	Mark Logsdon, CISO, NHS Digital • The issue of scale: delivering secure solutions to 1.5 million users • Embedding security in organisational structure • The implications of a truly risk-focused approach	
14:50	**Simplifying the path to Zero Trust through SASE**	
	Khalid Khan, Cybersecurity Strategist, Forcepoint • Understand how to successfully deploy Zero Trust with SASE for your business transformation • Discover the key steps to upgrading & migrating to a SASE stack for business wide adoption & optimisation • How to stay ahead of your threat actors with Zero Trust • Why risk reduction and dynamic protection is key • Demonstrate how to provide visibility and show business value.	
15:10	**How real is your security posture?**	
	Richard Ford, Chief Technology Officer, Integrity360 • Your security posture is only as good as the last time it was tested – will it protect you when you need it? • Real world case studies: those that have got it wrong, and how • How to assess & measure security effectiveness	
15:30	**Education Seminars | Session 3**	
	eSentire	**Building cyber-resilience by prioritising 24/7 threat detection and response** **Andy Lalaguna,** Senior Solutions Architect, eSentire
	Kiteworks	**The big 'why' of cybersecurity – reducing the risk of compliance violations and data loss on content shared with third parties** **Scott Chenery,** Regional Manager, and **Ben Readings,** Field Solutions Engineer, Kiteworks
	Noetic Cyber	**Building an effective threat & exposure management programme** **Chris Neely,** Director of Sales Engineering, Noetic Cyber
	Risk Ledger	**Defend as one – the new methodology for supply chain security** **Haydn Brooks,** CEO, Risk Ledger
	ZeroFox	**Ransomware: Tackling emerging and evolving threats in 2023** **Lewis Shields,** Principal Intelligence Analyst, ZeroFox
16:10	Networking break	
16:30	**FIRESIDE CHAT:**	**When security can't fail**
	Jesús Mérida Sanabria, CISO, Iberia • Guaranteeing security in a critical environment – lessons for the rest of us • Dealing with the changing threat landscape – prioritising material risk • The state of cybersecurity regulation • Is cybersecurity technology getting better?	
16:50	**EXECUTIVE PANEL DISCUSSION**	**CISO priorities discussion**
	Jane Corr, CISO, Canada Life Group Services Europe; **Darcy Delich-Coull,** CISO, Footasylum; **Simon Goldsmith,** Head of Information Security, OVO Energy; **Joseph Da Silva,** CISO, RS Group; **Jon Townsend,** CIO, National Trust • What would you say your top three priorities and challenges are – what challenges in your technology/people/process environments cause greatest problems for the information security programme? (eg. Hackers do seem to be targeting software build and test environments. Is this a weak link?) • How does legacy cybersecurity thinking and technology have to change to cope with almost random work patterns, demands for data portability? • Do you think that core security hygiene will soon be taken care of by things like a better version of the MS E5 licence, or security built into Google apps, plus the security built into your core Cloud apps and infrastructure? • How do you prioritise cybersecurity initiatives in the absence of any easy way to quantify cyber-risks? • Boards put cybersecurity in their top risk worries but to what extent are you under pressure to rein in the costs of cybersecurity? Are you under budget pressure? Is there pressure to outsource? • The cyber-talent shortage – real or illusion?	
17:30	Drinks reception	
18:30	End of Day 1	

Agenda | Day 2 | 2nd March 2023

08:00	Networking break	
08:50	Chairman's welcome	
08:55	**Ransomware, Russia and Regulation**	
	Irfan Hemani, Deputy Director of Cybersecurity and Digital Identity, Department for Science, Innovation and Technology • The current cyber-threat to the UK economy • Government's response • How businesses and organisations can take action to protect themselves	
09:10	**Software supply chain risk – What is it and why should you care?**	
	Michael White, Principal Architect, Synopsys • What the software supply chain looks like, exploring the anatomy of some these well-known software supply chain incidents • An overview of some key strategic initiatives that aim to support organisations in effectively identifying and managing software supply chain risk • How the efforts such as SBOM (Software Bills of Materials) are emerging • How to help cybersecurity organisations build awareness and resilience approaches, to improve mitigation and response strategies for software that they build, acquire, integrate, and depend upon	
09:30	**Is cyber-risk finally commanding the C-suite's attention?**	
	Johan Dreyer, Field Chief Technology Officer, Mimecast • The key findings from Mimecast's 7th annual study on 1700 Global IT and Cybersecurity Professionals • The State of Email Security report will cover the latest global insights on email-based cyber-threats, collaboration tools, cyber-preparedness and ways to reduce cyber-risk • The top 10 takeaways from the report to help deliver continuous improvements to your cyber-resilience strategy	
09:50	**Using past attacks to shape security and data protection strategy**	
	Sarah Lawson, CISO, UCL • Using the past to shape our cybersecurity future • What threat and attack data tells us about the processes and tools we need to target first • Practical choices for the resource-constrained CISO	
10:10	**Education Seminars | Session 4**	
	Forcepoint	**Defending your business from ransomware attacks** **Aaron Mulgrew,** Solutions Architect, Forcepoint
	Hoxhunt	**Human risk reduction – The big phishing game** **Sam Hooke,** Hoxhunt, and **Martyn Styles,** Head of Information Security, Bird & Bird LLP
	Integrity360	**Lessons from the frontline: Ransomware** **Richard Ford,** Chief Technology Officer, Integrity360
	Mimecast	**Getting the most from your cybersecurity investments: How to reduce complexity and lower costs** **Johan Dreyer,** Field Chief Technology Officer, Mimecast
	Obsidian Security	**SaaS backdoors – The risk of OAuth integrations for SaaS applications** **Ben Johnson,** CTO and Co-founder, Obsidian Security
	Searchlight	**A tour of dark web criminality and how to defend yourself** **Gareth Owenson,** Chief Technology Officer and Co-founder, Searchlight
10:50	Networking break	
11:20	**EXECUTIVE PANEL DISCUSSION**	**The fight against cybercrime – the importance of collaboration between government, law enforcement and industry**
	Simon Newman, CEO, The Cyber Resilience Centre for London (Moderator); **Eleanor Ludlam,** Partner, DAC BEACHCROFT; **Stuart Peters,** Head Cyber Resilience Policy Cybersecurity and Digital Identity Directorate, Department for Science, Innovation and Technology; **Jensen Penalosa,** Assistant Legal Attaché, FBI; **Andrew Gould**, Detective Chief Superintendent, National Cybercrime Programme Lead • What are government and policing doing to tackle the threat? • What can be done about low-reporting rates? Is it time to make it mandatory for everyone? • Is the law fit for purpose? What can we learn from elsewhere? • What can industry do to help policing and government?	
11:50	**See what they see, know what they know**	
	James Burchell, Senior Sales Engineer, CrowdStrike • To stop an adversary, you must first understand their tactics, techniques, and motivations. We have to adapt, fast! • Throughout 2022, CrowdStrike threat hunting activities covered record volumes of hands-on intrusion attempts with e-crime topping the charts • Adversaries continue shifting away from malware and continue to prove their unabating ability to adapt, splinter, regroup, and flourish in the face of defensive measures • However, 2022 also demonstrated that relentless determination works both ways • How organisations can prepare and protect themselves in this relentless threat landscape	

Agenda | Day 2 | 2nd March 2023

12:10 **'Global warning' a year of climate change on the threat barometer**

Adrian Jones, Country Manager UK & Ireland, Gatewatcher

- Join Gatewatcher as we compare two monthly snapshots from Gatewatcher's CTI Cyber Threat Barometer, February 2022 and 2023
- Sharing our insight into the changing target industries, attack vectors, types and techniques used
- Proffer some context and opinion across a 'year of warnings'

12:30 **Defending with an attacker's mindset**

Alistair Mills, Director, Sales Engineering, Proofpoint

The organisation chart is the new zero-day – and today, it's publicly available on social media

- It's easier to find someone who will click than to find an exploit for an operating system. The attacker simply needs to know who has access to the data they want, then get creative
- Most security teams don't have the same perspective that the threat actors do – they think of their attack surface in terms of VLAN and IP address, instead of department or job title
- Effective defence comes when you can anticipate your attackers' moves. By combining threat landscape insights with data on which of your users are targeted with which threats, organisations can build more effective security awareness training programmes, and users can better defend themselves from the threats they are most likely to see

12:50 **Education Seminars | Session 5**

BeyondTrust	**Cyber-threats: What you're up against & how to defend with PAM** **James Maude,** Lead Cybersecurity Researcher, BeyondTrust
Corelight	**Why network security monitoring? Why NDR? Why Zeek?** **Ashley 'AJ' Nurcombe,** Senior Cybersecurity Consultant – UK&I, Corelight
Gatewatcher	**Automate threat hunting, detection and incident response with NDR & CTI** **Ian Dutton,** Senior Sales Engineer, Gatewatcher, and **François Normand,** Cyber Threat Intelligence Manager, Gatewatcher
SentinelOne	**The myriad of security tools: How many is too many, what do I actually need and how do I develop a comprehensive security posture?** **PJ Norris,** Senior Security Engineer, SentinelOne
Transmit Security	**The power and peril of automation – How to flip the script on evasive bots and fraud** **Maurice Luizink,** Director, Solutions Engineering, Transmit Security

13:30 Lunch and networking break

14:30 **FIRESIDE CHAT: A CISO says**

Becky Pinkard, Head of Cyber Operations, Barclays

- Look on the bright side: progress in cybersecurity
- The real threat from nation states
- The truth about cyber-talent
- Getting information sharing right

14:50 **Get visibility and control over your attack surface**

Grant Revan, Head of Strategic Engagement, Red Sift

Explore how enterprise organisations can see, solve, and secure 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

15:10 **Preventing the single biggest unknown cybersecurity threats**

Jonathan Lee, Sr. Product Manager, Menlo Security

- Why current security solutions are failing to protect the remote workforce
- How modern work has given rise to Highly Evasive Adaptive Threats (HEAT)
- How HEAT attacks leverage phishing and malicious document techniques to dupe employees
- Understanding if your firm is susceptible to HEAT attacks and how to prevent them

15:30 Networking break

15:50 **FIRESIDE CHAT: A deep dive into building a quantitative technology risk programme**

Ash Hunt, CISO, Apex Group

- Why do CISOs and vendors keep talking about threats not risks?
- Defining realistic, measurable loss scenarios
- Filling the data gap: you have more than you think
- Lessons learnt and ROI conclusions

16:10 **Truth, lies and the slightly fuzzy nature of the dark web**

Adam Maxwell, Head of Information Security, Doctor Care Anywhere

- What content can you really find on the dark web?
- What are some of the misconceptions/truths about the dark web?
- What benefit can vendors bring to organisations specifically around dark web?

16:30 Drinks reception

17:30 Conference close

Education Seminars

Abnormal Security

More attacks, more problems: 7 key elements of effective email security

Dave Lomax, SE Director, EMEA, Abnormal Security

As long as companies use email, cybercriminals will launch email attacks. And as attackers continue to upgrade and enhance their strategies, it will become increasingly difficult for your employees to differentiate these threats from legitimate emails.

Because advanced email attacks exploit trusted email accounts and relationships, organisations need email security that can detect even small shifts in activity and content.

Join this session with Abnormal Security for insight into:

- Why modern and sophisticated attacks evade traditional solutions
- Real-world examples of inbound email attacks and email platform attacks
- The key essentials for effective cloud email security
- And what you can do to protect your organisation from the threats of today – and the future

BeyondTrust

Cyber-threats: What you're up against & how to defend with PAM

James Maude, Lead Cybersecurity Researcher, BeyondTrust

Cyber-threats shows no signs of abating. Digital transformation, expanding cloud deployments, and increased remote work are all bolstering the attack chain, creating new planes of privileges for attackers to exploit. Breaking the chain is more vital than ever. Despite this, organisations continue to mishandle projects, leaving themselves at significant risk of attack.

Following the overview on the main stage, join James Maude as he takes a deeper dive into exploring how to break the chain with PAM:

- Common attack chain entry points
- Practical steps you can take to block entry
- How PAM ensures project success

Cisco

Why productivity and security need to be two sides of the same coin

Rob Lay, Leader, Systems Engineering, Cisco

While security teams work to stay vigilant and put defences in place, how can we balance this with high productivity and low friction? User experience should not be the sacrificial lamb. If productivity takes a hit, then security is seen as the bad guy in the organisation, even within IT teams.

At the same time as people and organisations find innovative ways to transform digitally, we also see attackers finding new and creative ways to circumvent security controls. Protecting against attacks that bypass authentication and compromise users is now a heightened priority.

Cisco Secure looks at some typical user journeys, referencing security at the backend and how we keep this quietly effective.

- Where is the market?
- End user experience versus security
- User journeys and backend operation
- Security uplift
- Summary

Corelight

Why network security monitoring? Why NDR? Why Zeek?

Ashley 'AJ' Nurcombe, Senior Cybersecurity Consultant – UK&I, Corelight

NDR provides continuous network security monitoring capability to find evidence of malicious activity. This course will help network defenders understand the gold standard of network telemetry to fuel threat hunts and incident response.

- Describe the types of data to collect for network monitoring
- Differentiate Zeek data from traditional data collection
- Walk through use cases, demonstrating how Zeek data helps resolve issues faster than traditional tools
- Explain the positives and negatives of open and closed source monitoring tools.

Education Seminars	
CrowdStrike **The external attack surface is constantly changing. How can you identify unknown risks and exposures in real time?** **James Burchell,** Senior Security Engineer, CrowdStrike	• How can you identify unknown risks and exposures in real time? • Demystify EASM: What is it? Why is it important? And why now? • Understand how to leverage EASM capabilities and reduce exposure risk from the outside-in to the inside-out
eSentire **Building cyber-resilience by prioritising 24/7 threat detection and response** **Andy Lalaguna,** Senior Solutions Architect, eSentire	In today's threat landscape, security leaders must shift their focus to improving their cyber-resilience. The ability to anticipate, withstand, recover from, and adapt to the evolving cyber-threats will dictate how well-equipped your cybersecurity programme is at defending against these threats. However, given the lack of skilled in-house security resources, it can be challenging to balance the number of incoming security alerts with delivering swift response to eliminate known and unknown threats. In this presentation, join Andy Lalaguna, Senior Solutions Architect at eSentire, as he shares insights on how you can leverage 24/7 threat detection, investigation, and response capabilities to reduce your cyber-risk, build resilience and prevent business disruption. Key takeaways include: • How to assess, understand, and quantify your cyber-risks • Why you should shift your focus to building cyber-resilience in addition to managing your cyber-risks • How proactive threat hunting, combined with 24/7 threat detection and response, are critical in developing a strong cyber-defence strategy
Forcepoint **Defending your business from ransomware attacks** **Aaron Mulgrew,** Solutions Architect, Forcepoint	Ransomware attacks are evolving and growing in sophistication. It seems likely that the criminals are ploughing their profits back into the tools and platforms they use. They are building expertise and targeting high-profile organisations, confident in the knowledge that they are increasingly successful. Combatting this problem requires additional defences that offer advanced protection. The increasing agility of criminal groups point toward why prevention-based defences are becoming rapidly more popular. • Discover the best ways to defend your business from the most popular ransomware threats in 2023 • Understand the step-by-step approach to combatting the threat
Gatewatcher **Automate threat hunting, detection and incident response with NDR & CTI** **Ian Dutton,** Senior Sales Engineer, and **François Normand,** Cyber Threat Intelligence Manager, Gatewatcher	Cyber-threats against organisations of all sizes and across all verticals are increasing in volume and in sophistication. It is therefore necessary to ensure that efficient and effective technologies are in place to quickly detect and remediate attacks. Learn how this can be achieved by combining the latest cyber-threat intelligence with network detection and response. • Learn how integrating CTI and NDR technologies enables rapid detection and response against the latest advanced cyber-threats • Understand both realtime and retrospective hunting capabilities of NDR and CTI • Gain insight into the enhanced detection capabilities for APT and zero days

Education Seminars

Hoxhunt **Human risk reduction – the big phishing game** **Sam Hooke,** Sales Director, Hoxhunt, and **Martyn Styles,** Head of Information Technology, Bird & Bird LLP	Gartner's recent Insight report identified that over 90% of cybersecurity functions have an awareness programme, yet 69% of employees admit to intentionally bypassing their enterprise's cybersecurity guidance during the past year. How do you address these engagement levels and reduce the human risk of phishing? In this session, we will explore with Martyn Styles Head of Information Technology, Bird & Bird LLP: • Approaches for behavioural and cultural change to create a more cyber-aware and engaged workforce • How better management & reporting has helped reduce the human risk • How these changes have improved their overall cybersecurity posture from board-level and across the whole organisation • Overview of Hoxhunt capabilities
Integrity360 **Lessons from the frontline: Ransomware** **Richard Ford,** Chief Technology Officer, Integrity360	Ransomware is by far the biggest cyber-threat to businesses, threatening operations, productivity, brand/reputation and finances. Ransomware has evolved. Not only in the way it impacts and extorts organisations but also in the methods used to become the super-threat it is today. Continued success of ransomware is fuelling growth in attacks, and current mitigation strategies are not working, and leaving organisations vulnerable. In this seminar, we'll go to the frontline with Integrity360's Incident Response team to look at lessons from the field, and the learnings that can put us all in a better position in the fight against ransomware: • Three real-world case studies of ransomware incidents • End-to-end timeline from attack to extortion, and how these incidents played out • Actionable takeaways on the lessons learnt and advice on how to prepare your organisation should the worst occur
Intel 471 **The seven habits of effective cybercriminals** **Maurits Lucas,** Director of Product Marketing, Intel 471	As the impact of cyber-threats to businesses and governments across the globe keeps increasing, it is more important than ever to understand how threat actors and groups operate in the cyber-underground and in particular how they maintain their effectiveness. In this session, we will: • Look at what makes certain actors or groups so successful • By increasing our understanding of the social patterns and psychological traits of these individuals – an area of cybersecurity often overlooked – attendees will be able to improve mitigation efforts by anticipating how future threat actors will exhibit specific characteristics and how their successes influence others to adopt similar strategies • Present the results of analysis of more than 12 years of tracking and reporting on a variety of actors and groups in the cyber-underground that allowed us to identify seven specific habits of highly effective actors and groups that we will present, along with examples illustrating each of these habits
Kiteworks **The big 'why' of cybersecurity – reducing the risk of compliance violations and data loss on content shared with third parties** **Scott Chenery,** Regional Manager, and **Ben Readings,** Field Solutions Engineer, Kiteworks	Do you feel confident you have complete command of all your sensitive information as it is sent or shared, no matter the communication channel? Or are you – like many C-level decision makers – struggling with the reality of disparate systems, poor tracking, little to no control, and weak security when it comes to governing and securing your sensitive content when being shared externally? Join this practical session with Kiteworks for insights on: • Why organisations are so concerned around content governance and security • How you can reduce risk using zero trust principles when doing business with third parties • What does the future hold in content sharing – The PCN Framework • Unifying, tracking, controlling and securing content across email, file sharing, APIs, etc.

Education Seminars

Menlo Security

The next class of browser-based attacks

Tom McVey, Solution Architect, Menlo Security

There are two distinct characteristics that all threat actors tend to share. First, they focus on avoiding detection by any means. Second, while some go after specific targets, many opt to aim their tactics at the vectors that will reap the greatest rewards. After all, a big pond with many fish increases everyone's chances of success.

Between July and December 2021, there was a 224% increase in highly evasive adaptive threats (HEAT) attacks – a class of cyber-threats targeting web browsers as the attack vector. While malware once had to be downloaded to pose a real risk, now, it's a dynamically generated threat toolkit built in the web where employees are productive.

In this session, you will:

- Discover the anatomy of recent browser-based attacks
- Learn why network security today is broken
- Experience a live demo that enables you to discover the technology approach proven to eliminate these threats

Mimecast

Getting the most from your cybersecurity investments: How to reduce complexity and lower costs

Johan Dreyer, Field Chief Technology Officer, Mimecast

2023 will bring more cyber-attacks, of higher sophistication, at a time of increased vulnerability, where businesses are having to evaluate spend on new and existing cybersecurity tools as the global economic climate cools and rate hikes slow organic growth. The technology complexity and sophistication are keeping organisations from making measurable progress against cyber-attacks. Yesterday's cyber-defences will no longer protect against the elevated risks to people, communications, and data. So, security systems will necessarily grow more intelligent and orchestrated, but added challenges such as today's cybersecurity skills shortage will likely delay that much-needed progress.

In this session, we will look at:

- Trends & takeaways from the 2022 threat landscape
- How to balance budget constraints with growing security challenges
- Overcoming the technical debt of legacy security systems
- Utilising managed services to bridge the skills gap to help better protect your organisation, brand and reputation

Noetic Cyber

Building an effective threat & exposure management programme

Chris Neely, Director of Sales Engineering, Noetic Cyber

An important area of focus for security leaders is managing and reducing their attack surface and level of exposure. To do that, they need to understand what assets they have and the risk they pose to the business.

Shifting trends in modern business have resulted in an explosion in digital assets across the cloud, SaaS applications and remote devices. Security teams needs to know what they have, what could be the impact of a breach, and what security controls are in place to mitigate that risk.

In this session, delegates will learn:

- The essential building blocks to build an effective Continuous Threat Exposure Management (CTEM) programme
- Best practices on leveraging existing security and IT data sources to map cyber-relationships and risk across the organisation
- How to identify security coverage gaps and 'toxic combinations' relevant to your business
- How to better prioritise security workload through clearer understanding of business context and criticality
- Industry best practice on how to implement a CTEM programme in your organisation

Education Seminars	
Obsidian Security **SaaS backdoors - the risk of OAuth integrations for SaaS applications** **Ben Johnson,** CTO and Co-founder, Obsidian Security	Today, leading SaaS applications like Microsoft 365, Google Workspace, and Salesforce effectively function as centralised platforms accessed by a sprawling number of interconnected integrations and APIs. While the productivity benefits of these connections are clear, the security risks they introduce are often overlooked. SaaS-to-SaaS integrations are often the largest conduit for data movement within organisations so it's no surprise that threat actors are increasingly exploiting this interconnection. High-profile breaches like Sunburst or more recently involving GitHub, highlight the lack of visibility organisations have into such threats. • In this threat briefing, Obsidian Co-founder and CTO Ben Johnson explores security considerations around SaaS integration risk, shares some firsthand findings from our customer base, and provides some guidance on how to address these vulnerabilities
Ontinue **SecOps automation in Microsoft Teams?** **Drew Perry,** Chief Innovation Officer, Ontinue	Do you collaborate with your MSSP or SOC provider in real-time? Have you automated Tier 1 analysts? Do your cyber-defenders have time to threat hunt? • Learn about the 'collaboration & automation' security operations mindset • Create a force multiplier to prevent cyber-incidents • The SecOps world has changed, AI is here... are you ready for it?
Proofpoint **Rethink your approach to data loss prevention** **Richard Combes,** Senior Manager – Technical Sales, Proofpoint	Data doesn't lose itself – people lose data. Whether an employee is careless when handling and moving your data, has malicious intent to take data with them when leaving to a different employer or their account credentials have been compromised by an external attacker, it is important to have visibility into the risk presented by any of these scenarios. Yet legacy DLP technology just hasn't lived up to its promises. So what can you do when you are only looking at content and when your classification of data is not on a par with modern standards? It is time to rethink your strategy to protecting your sensitive data, including intellectual property and PII. Let an industry player trusted by almost half of the Fortune 100 guide you. In this talk, you will gain an understanding of: • What a modern information protection strategy looks like • How to classify data to build effective protection • Identify who is moving what data, when, where and why • Detect risky insiders, especially those exiting your organisation • Prevent data loss across multiple channels including cloud and email
Red Sift **Protect your digital brand in 2023** **Jorge Montiel,** Head of Sales Engineering – EMEA, Red Sift	In this session, Jorge Montiel, Head of Sales Engineering for EMEA at Red Sift, offers insights into the evolution of cyber-attacks and brand abuse on enterprise organisations, and how you can defend your brand against these. He will cover: • The changing nature of impersonation attacks and domain abuse, and how fraudsters are achieving their goals • What steps organisations can take to protect themselves now and for the future • How organisations are defending their brands against impersonation while building consumer confidence and positively influencing buyer behaviour

Education Seminars

Risk Ledger

Defend as one – the new methodology for supply chain security

Haydn Brooks, CEO, Risk Ledger

Ovr the last decade supply chains have become increasingly interconnected, something which attackers have exploited (60% of organisations have suffered a security breach through a third party). The status quo for managing these problems has quickly become outdated and a new methodology is needed, the NHS has started utilising the 'defend as one' mentality, where they work with their suppliers to strengthen their security.

In this talk, Haydn Brooks will discuss, the status quo or running a TPRM programme, what's changed and how a new methodology will help keep the global supply chain secure.

Key points:

- The status quo of running a TPRM programme
- The pros and cons of the current approach
- What's changed/why do we need a new methodology?
- How the new defend as one methodology works
- What the next 10 years looks like

Searchlight Cyber

A tour of dark web criminality and how to defend yourself

Gareth Owenson, Chief Technology Officer and Co-founder, Searchlight

- Real-life examples of cybercriminal activity that can be observed on dark web forums, marketplaces and sites
- How organisations can gather threat intelligence on criminals targeting their organisation before they strike
- How this 'pre-attack' intelligence can be actioned as part of an organisation's cyber-defence
- Practical steps defenders can take to improve their understanding and response to dark web threats

SentinelOne

The myriad of security tools: How many is too many, what do I actually need and how do I develop a comprehensive security posture?

PJ Norris, Senior Security Engineer, SentinelOne

XDR, EDR, Cloud, user behaviour, threat hunting, identity protection, access management – ARGH! In today's world, we are seeing an ever-increasing amount of new security tools (and new security acronyms!) promising to alleviate all of those 'demons keeping you up at night'. Each month seems to bring us a new 'latest and greatest'.

Join SentinelOne as we discuss;

- In the ever-evolving world, what really are the key technologies we need to invest in to keep our infrastructure safe?
- How do we even begin to think about properly building out a comprehensive security stack?
- What are the fundamentals any security team should look to implement in order to stay ahead of tomorrow's adversary?

Silobreaker

Tools and tactics to solve the top 3 Open-Source Intelligence (OSINT) challenges

Kevin Tongs, Account Executive, Silobreaker

Open-Source Intelligence (OSINT) has become increasingly important to organisations looking to identify potential risks and vulnerabilities early, whether phishing, malware or the latest ransomware attack. Join Silobreaker in this talk to learn the tools and tactics to solve the top 3 open source intelligence challenges, and respond more quickly to attacks that put your organisation at risk.

- Shift from a manual approach and automate data collection and aggregation to save time and uncover critical intelligence at speed
- Determine Open-Source accuracy, credibility, timeliness, and objectivity more efficiently and effectively to keep your organisation safe from risk
- Make faster, more relevant connections between different types of risk intelligence to gain strategic advantage when responding to threats

Education Seminars

Synopsys

From SCA, to software supply chain risk management to SBOM

Matthew Brady, Sales Engineering Manager, Synopsys

If you're among those struggling to prioritise your supply chain risk efforts, Synopsys can guide you through the journey from Software Composition Analysis (SCA) to Software Supply Chain Security and SBOM management.

In this seminar, we'll discuss the current buzz around:

- Software Bills of Materials (SBOMs)
- Software supply chains, along with the evolving software security requirements in the US and EU
- How organisations remain unprepared to handle new vulnerabilities in open-source software, such as Log4J

Transmit Security

The power and peril of automation – how to flip the script on evasive bots and fraud

Maurice Luizink, Director, Solutions Engineering, Transmit Security

There is nothing like a true story to show the business value of AI-powered fraud protection – as you saw in our keynote on ChatGPT. In this case, a leading US bank was attacked by registration bots that created thousands of fake new accounts. The attackers went to great lengths to evade detection, such as using unique IP addresses for each account. Clever, but what we saw next was far more surprising and would enable the bots to slip past most bot and fraud defences.

In this educational session, we'll show you:

- How the fraud landscape is becoming far more challenging due to sophisticated obfuscation techniques attackers use to go undetected
- Why you now need to leverage a variety of real-time risk signals to stand a chance
- Staying ahead of the attacker curve: How you can detect bot attacks much sooner – long before you see a spike in traffic
- Use AI & ML to your advantage: How to leverage ML and AI to improve the accuracy of fraud detection and automate your decisioning

VMRay

Getting sand in funny places: Understanding malware sandboxing

Michael Bourton, Senior Security Solutions Engineer EMEA & APAC, VMRay

Over the past decade, sandboxes have become the standard tool for the analysis of previously unseen malware. They are embedded in security controls such as NGFWs, email- and web-gateways, play a role in EDR, XDR, SOAR and SIEM implementations, and are widely used for incident response and threat hunting.

Therefore, you may already have a sandbox in your security environment, but what exactly is it for, how does it work and does it really protect you?

In this session, we will take a closer look at a technology you may have ignored. Join us for a deep-dive into sandboxing and learn how to stop worrying and love your sandbox.

We will cover:

- Background on common points and common technology
- Avoidance techniques
- Benchmarking
- Sharing IoCs

ZeroFox

Ransomware: Tackling emerging and evolving threats in 2023

Lewis Shields, Principal Intelligence Analyst, ZeroFox

As businesses remain focused on strengthening internal security, threat actors continue to exploit opportunities beyond the perimeter.

In 2022, ransomware and digital extortion remained some of the most significant cyber-threats to organisations in most sectors and locations globally, which was likely caused partly by geopolitical events and increased difficulty eliciting payments from victims.

Join this session to explore:

- Insights on ransomware and digital extortion threats in 2022
- Forecast and recommendations to help security teams tackle evolving ransomware threats in 2023 and beyond
- How global events like the war in Ukraine have impacted cybercrime