Post event report

Strategic Sponsors

BeyondTrust
BEYOND IDENTITY
CROWDSTRIKE
DARKTRACE
illumio
imperva
MENLO SECURITY
NETACEA
okta
proofpoint.
Recorded Future®
RED SIFT
SENSE ON
TESSIAN

Education Seminar Sponsors

data SOLUTIONS
CEQUENCE SECURITY
COFENSE
CybelAngel
cybersixgill
DEVO
FIREMON
helpsystems
INTEL471
CISCO | KENNA Security
ManageEngine
OPSWAT.
PICUS
Synack
VECTRA

Branding Sponsors

C2 CYBER LTD RESILIENCE REALISED
ORCHESTRA
TELESOFT

"What a fantastic week we had because of your conference!"
Head of Cyber Crime Partnerships, Bank of America

"It was fantastic and all the information and presentations were very informative and educational. Thank you for organising this, it is just mind opening."
IT Manager, Trinitas Academy Trust

"Once again the e-Crime & Cybersecurity Congress was both insightful and educational, providing great networking opportunities, allowing sharing from across verticals."
Head of Information & Cyber Security, McArthurGlen Group

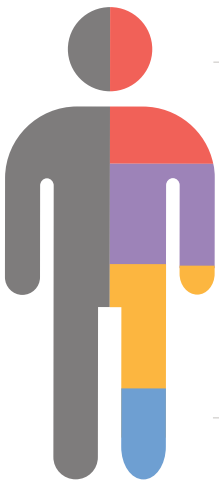
"Good to be back to an in-person meeting, great presentations and shared insights between fellow attendees."
Senior Information Security Consultant, Phoenix Group

Inside this report:

Key themes

- Where's the government when you need it?
- From cybercrime to cyberwar
- 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 - really
- From smart machines to smart cities – securing the IoT
- All aboard the Cloud
- Getting real about automation, AI and the rest
- 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

Tim Ager, VP of Sales, EMEA, Picus Security; Ruth Anderson, Director Group Operational Resilience and Security, Lloyds Banking Group; Pal Balint, Senior Sales Engineer, Imperva; Ed Bishop, Chief Technology Officer and Co-founder, Tessian; Lewis Brand, Senior Sales Engineer, Recorded Future; Elaine Bucknor, Group CISO and Group Director, Technology Strategic Services, Sky Plc; James Burchell, Senior Security Engineer, CrowdStrike; Prakhar Chandra, BISO, News UK; Greig Sharman, Chief Technology Officer, NSPCC; Brian Chappell, Chief Security Strategist (CSS), EMEIA & APAC, BeyondTrust; Nick Coleman, Chief Security Officer for Real-Time Payments, Mastercard; Pete Cooper, Deputy Director Cyber Defence, UK Cabinet Office; Steve Cottrell, EMEA CTO, Vectra; Trevor Dearing, Director of Critical Infrastructure Solutions, Illumio; Eleanor Fairford, Deputy Director for Incident Management, NCSC; Brad Freeman, Director of Technology, SenseOn; Simon Goldsmith, Director for Information Security, OVO Energy; Matthew Gracey-McMinn, Head of Threat Research, Netacea; Nipun Gupta, Cybersecurity Specialist, Devo Inc; Adam Gurney, Sales Engineer, OPSWAT; Mary Haigh, CISO, BAE Systems; Nick Hogg, Director of Technical Training, HelpSystems; Federico Iaschi, BISO, Virgin Media O2; Neil Johnson, Head of Security and Threat Solutions, TikTok; Vijay Kishnani, Lead Cyber Security Engineer, CybelAngel; Major General Ben Kite, Director of Intelligence Interoperability, Ministry of Defence; Zibby Kwecka, Head of Information Security, Heineken UK; Fred Langford, Director Online Technology, OFCOM; Jonathan Lee, Senior Product Manager, Menlo Security; Toby Lewis, Head of Threat Analysis, Darktrace; Bryan Littlefair, CISO & Cybersecurity Consultant, presenting on behalf of FireMon; Ian Lowe, Director of Solutions Marketing, EMEA, Okta; Maurits Lucas, Director of Product Marketing, Intel 471; Ciaran Martin, Professor of Practice in the Management of Public Organisations, Blavatnik School of Government at Oxford University; Neil McRae, Solution Engineer, Tessian; Alistair Mills, Director, Sales Engineering, Northern Europe, Proofpoint ; Raghu Nandakumara, Head of Industry Solutions, Illumio; Andy Ng, Partner, Cyber, EY Consulting; Isaac Ng, CISO, Southeastern Railway; Cyril Noel-Tagoe, Cyber Threat Evangelist, Netacea; Jensen Penalosa, Assistant Legal Attaché, FBI; Dr Rois Ni Thuama, Head of Cyber Governance, Red Sift; Benjamin Preminger, Product Manager, Cybersixgill; Helen Rabe, CISO, Abcam; Brett Raybould, Head of Solutions (EMEA), Menlo Security; Jill Robertson, Head of Information Security Change Team, Metro Bank; Chris Robins, Senior Sales Engineer, EMEA, Beyond Identity; Stephen Roostan, VP, EMEA, Kenna Security; Alain Salesse, Senior Sales Engineer, Cofense; Ian Shaw, Head of Risk and Security, South East Coast Ambulance Service, NHS Foundation Trust; Justin Shaw-Gray, Sales Director for UKI and South Africa, Synack; James Sherlow, Systems Engineering Manager, EMEA, Cequence Security; Eric Smithmier, Assistant Legal Attaché, FBI London, Cyber Division; Jason Steer, Principal Security Strategist, Recorded Future; Danielle Sudai, Cloud Security Operations Lead, Deliveroo; Crawford Thomas, Global Head of Cyber Threat Intelligence, Credit Suisse; Ian Tinney, CEO, 4Data Solutions; Jon Townsend, CIO, National Trust; Ram Vaidyanathan, Cyber Risk and Security Expert, ManageEngine; Chris Waynforth, Area VP, EMEA North, Imperva; Mark Walmsley, Chief Information Security Officer (CISO), Freshfields Bruckhaus Deringer LLP; Lee Whatford, CISO, Domino's Pizza; David Whitelegg, European Security Officer, Compass Group; Engin Yilmaz, Product Director, Red Sift

Agenda | Day 1 | 2nd March 2022

08:00 **Registration and breakfast networking**

08:50 Chairman's welcome

09:00 **Securing the citizen (patient, employee, tax-payer…..)**

Eleanor Fairford, Deputy Director for Incident Management, NCSC

- The current threat level and significant threat types/actors
- Lessons learned from the attacks of 2021
- Advice for public and private sector organisations looking to improve their cyber-resilience

09:20 **The path to zero trust with least privilege & secure remote access**

Brian Chappell, Chief Security Strategist (CSS), EMEIA & APAC, BeyondTrust

- What zero trust is and how NIST defines it
- The goals of zero trust
- Roadblocks to zero trust (legacy architectures and technologies)
- How Privileged Access Management aligns with and enables zero trust

09:40 **Following threat actor bread crumbs**

James Burchell, Senior Security Engineer, CrowdStrike

The e-crime ecosystem is an active and diverse economy of financially motivated threat actors that engage in a myriad of criminal activities in order to generate revenue. Join this session to:

- Take a deep dive into notable shifts in advanced adversary operations
- Get an understanding of how monitoring of this malicious ecosystem is critical for
  - Early detection
  - Preventing expensive data compromises and ransomware incidents…

…No matter how big or small your security team is

10:00 **The real battleground of cybersecurity**

Ciaran Martin, Professor of Practice in the Management of Public Organisations, Blavatnik School of Government at Oxford University,

- What government defences can stop and what they cannot (so what is left for private sector CISOs to deal with)
- How the national security response is evolving and how our cybersecurity as a nation is improving/getting worse
- How our cybersecurity resilience is impacted by reliance on a few foreign providers of core infrastructure (Cloud)
- The level of cybersecurity investment by government and the private sector – adequate/inadequate?
- How private sector security solutions are/are not helping improve security and resilience

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

Beyond Identity	**Beyond Identity's Passwordless MFA: The only way to positively verify user identity at login** **Chris Robins,** Senior Sales Engineer, EMEA, Beyond Identity
Devo	**Single source of truth – the fundamental building blocks for an effective security operations centre** **Nipun Gupta,** Cybersecurity Specialist, Devo Inc
Imperva	**APIs as your ultimate honeypot** **Pal Balint,** Senior Sales Engineer, Imperva
Netacea	**BLADE: Cutting through the complexity of business logic attacks** **Matthew Gracey-McMinn,** Head of Threat Research, Netacea, & **Cyril Noel-Tagoe,** Cyber Threat Evangelist, Netacea
Recorded Future	**The business of fraud: Sales of PII and PHI** **Lewis Brand,** Senior Sales Engineer, Recorded Future
Red Sift	**Why building a people-first security culture is the key to cyber-defence in 2022** **Engin Yilmaz,** Product Director, Red Sift
SenseOn	**Root cause analysis in moments, not days** **Brad Freeman,** Director of Technology, SenseOn

11:00 Networking and refreshments

11:30 **Building the UK as a global responsible cyber-power – the part industry plays**

Mary Haigh, CISO, BAE Systems

- The importance of agility and creativity in cybersecurity. To achieve stable, robust growth through digital transformation we must have resilient infrastructure that is secure by design. I will explore what this means in reality and how we can address the 'responsible' aspect of cyber-power in industry
- Agility and creativity requires a higher level of digital literacy and cyber-expertise. I will look at how that can be nurtured in organisations
- The challenge of delivering cybersecurity in large organisations. Building scalable systems requires a careful balance of central visibility and control with agile local decision making

11:50 **Stopping ransomware with Autonomous Response**

Toby Lewis, Head of Threat Analysis, Darktrace

- Recent ransomware threat trends, including double extortion and RDP attacks
- How Autonomous Response takes action to contain an emerging attack, even when security teams are out of office
- Real-world examples of ransomware detected by Darktrace AI – including a zero-day and an attack initiated on Christmas Day

12:10 **Accelerating digital transformation: How to reduce friction in every digital experience**

Ian Lowe, Director of Solutions Marketing, EMEA, Okta

- Find out how to strengthen your security posture
- Learn about the challenges we are facing when it comes to securing a dynamic workforce
- Deep dive into current case studies on how to reduce IT friction in identity

12:30 **Protecting people: The new perimeter**

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

- Why social engineering dominates among today's cyber-threat actors
- How remote work and the move to the cloud has changed the nature of threats
- The ways organisations are building controls to better understand and protect people

Agenda | Day 1 | 2nd March 2022

12:50 Education Seminars | Session 2

ManageEngine	**How to use the MITRE ATT&CK framework to stop ransomware** **Ram Vaidyanathan,** Cyber Risk and Security Expert, ManageEngine
Okta	**How identity can accelerate digital trust** **Ian Lowe,** Director of Solutions Marketing, EMEA
Picus Security	**The CISO's challenge – how to be more proactive with less** **Tim Ager,** VP of Sales, EMEA, Picus Security
Synack	**Hacking for the greater good: Using hackers to beat hackers** **Justin Shaw-Gray,** Sales Director for UKI and South Africa, Synack, & **Mark Walmsley,** Chief Information Security Officer (CISO), Freshfields Bruckhaus Deringer LLP
Tessian	**Master defence in depth: Supercharging the security of your Microsoft email environment** **Neil McRae,** Solution Engineer, Tessian
Vectra	**How AI based 'Threat Detection & Response' finds and stops ransomware** **Steve Cottrell,** EMEA CTO, Vectra

13:30 Lunch and networking

14:30 EXECUTIVE PANEL DISCUSSION – Getting cybersecurity regulation right

Andy Ng, Partner, Cyber, EY Consulting; **Fred Langford,** Director Online Technology, OFCOM; **Elaine Bucknor,** Group CISO and Group Director, Technology Strategic Services, Sky Plc; **Federico Iaschi,** BISO, Virgin Media O2

- Should regulators create more cybersecurity specific regulations instead of the current focus on data privacy?
- Is regulating the resilience of CNI perhaps a better way to address the problem of cybersecurity?
- What about the IoT? Is regulating operational technology feasible?
- How can regulators work more closely with both legislators and industry to come up with useful standards to help secure economies and society?

14:50 Why human layer security is the missing link in enterprise security

Ed Bishop, Chief Technology Officer and Co-founder, Tessian

- Email is every bit as crucial an environment to protect as the network and databases; once compromised, there can be lasting, costly, and damaging effects. Leaning on built in security controls of email platforms or legacy technology are insufficient in providing comprehensive protection against human-related threats over email
- Over 75% of firms report that 20% or more of email security incidents get past their existing security controls
- The findings from the commissioned study conducted by Forrester Consulting on behalf of Tessian recommends that organisations consider human layer security to be used
- Learn how human layer security technology will help you to feel more prepared to face email security threats and data loss incidents (accidental, negligent, or malicious) and demonstrate a higher level of maturity when it comes to readiness to prevent these damaging threats
- Learn how human layer security technology will increase your visibility into risky behaviour, automate threat detection and prevention, save your organisation from reputation damaging data breaches and hours of resource time monthly, and set you up for email security success with a focus on in-the-moment security coaching and preventative technology

15:10 HEAT attacks: Examining the next class of evasive, adaptive web threats

Jonathan Lee, Senior Product Manager, Menlo Security

- How has modern work given rise to HEAT attacks?
- What delivery mechanisms do these attacks leverage to evade detection?
- The impact of HEAT attacks on organisations of all sizes and sectors
- What can organisations do to prevent HEAT attacks?

15:30 Education Seminars | Session 3

CrowdStrike	**How to reveal secrets from criminal forums and interrupt adversaries in their tracks** **James Burchell,** Senior Security Engineer, CrowdStrike
CybelAngel	**Finding the leaky data links in your supply chains – data security beyond perimeters** **Vijay Kishnani,** Lead Cyber Security Engineer, CybelAngel
HelpSystems	**HelpSystems Data Security Suite: Protecting your data with layered security solutions** **Nick Hogg,** Director of Technical Training, HelpSystems
Kenna Security	**Cisco SecureX + Kenna Security: Radical simplification in the new era of cybersecurity** **Stephen Roostan,** VP, EMEA, Kenna Security
OPSWAT	**File upload protection: A critical gap in web app security** **Adam Gurney,** Sales Engineer, OPSWAT

16:10 Networking and refreshments

16:30 EXECUTIVE PANEL DISCUSSION – CISO priorities for 2022

Danielle Sudai, Cloud Security Operations Lead, Deliveroo; **Prakhar Chandra,** BISO, News UK; **Greig Sharman,** Chief Technology Officer, NSPCC; **Isaac Ng,** CISO, Southeastern Railway; **Neil Johnson,** Head of Security and Threat Solutions, TikTok

- Data privacy or security? How will companies view 'security' in the post-pandemic world?
- Hybrid working: problem solved or problem postponed?
- Is 2022 the year of Cloud? And have the security implications of Cloud been exaggerated?
- The future of the security stack

16:50 Towards better cyber-resiliency: Digital transformation with risk reduction

Raghu Nandakumara, Head of Industry Solutions, Illumio

- See how the attack surface is growing as technology use is changing
- Understand why a Zero Trust approach is essential to reducing this risk
- Identify how better security can be incorporated into your transformation

17:10 Engaging with the board – getting the backing, finding the finance

Lee Whatford, CISO, Domino's Pizza

- Why it's all about risk, or is it? Using the right language
- Shifting the tone – from IT security to business risk management
- Framework ideas – quantifying the ask

17:30 Networking and drinks reception **18:30** End of day one

Agenda | Day 2 | 3rd March 2022

08:00 Registration and breakfast networking

08:50 Chairman's welcome

09:00 **Driving change at scale**

Pete Cooper, Deputy Director Cyber Defence, UK Cabinet Office

Pete has led and worked across global communities and driven change at scale, most recently on the first ever Government Cyber Security Strategy. In this talk he will walk through:

- The key approaches to success at scale
- Managing sectoral changes
- Developing scalable cybersecurity strategies

09:20 **Malicious bot attacks are becoming ever more frequent, and high profile**

Matthew Gracey-McMinn, Head of Threat Research, Netacea, & **Cyril Noel-Tagoe,** Cyber Threat Evangelist, Netacea

- Malicious bot attacks are becoming more frequent and high profile, with a slew of scalper bot attacks hitting the headlines since 2020, as attackers target in-demand items such as the Playstation 5 and even Covid-19 vaccine appointments
- According to Netacea's recent survey, 46% of enterprise organisations had experienced an account takeover attack in 2020. 58% of these businesses stated that the attacks had a known financial impact
- During our session, we will explore the scale of the account takeover attack problem, zoning in on credential stuffing and how these attacks are executed, with a live demonstration using real attacker tools
- We will then walk through the makeup of attacker tooling, explaining how they bypass defences and how they maximise the efficiency of their attacks
- We will discuss the impact on various sectors, including retail, telecommunications and financial services

09:40 **Why SOCs fail**

Brad Freeman, Director of Technology, SenseOn

- Poor SOC technology implementations critically hamper both people and processes, which leads to SOC failure
- Developing an efficient SOC is an engineering challenge. Bringing together tools, data and in house engineering to deliver a tailored solution specific business outcomes
- Hard learned lessons of implementing security operations. Insights into when they work well, when they don't, and why they don't
- Reveal of technology innovations relating to breakthroughs of unified telemetry and how it can change security operations

10:00 **Defence perspectives on future trends of cyber and e-crime**

Major General Ben Kite, Director of Intelligence Interoperability, Ministry of Defence

- Introduction and exploration of the breeding grounds for cyber-actors and threats they pose
- The unique cyber-challenges for defence
- How will technology change criminal behaviour?

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

4Data Solutions	**Observability; a data driven approach to cloud security** **Ian Tinney,** CEO, 4Data Solutions
Cequence Security	**Frictionless API security strategies** **James Sherlow,** Systems Engineering Manager, EMEA, Cequence Security
Cofense	**Adaptive email security architecture: Moving from incident response to continuous response** **Alain Salesse,** Senior Sales Engineer, Cofense
Cybersixgill	**Chihuahuas VS. muffins: Developing AI solutions for threat intelligence problems** **Benjamin Preminger,** Product Manager, Cybersixgill
Darktrace	**Fast and furious attacks: Using AI to surgically respond** **Toby Lewis,** Head of Threat Analysis, Darktrace
Intel 471	**Back to the future** **Maurits Lucas,** Director of Product Marketing, Intel 471

11:00 Networking and refreshments

11:30 **'Threatcasting' looking and preparing for threats up to 10 years out**

Nick Coleman, Chief Security Officer for Real-Time Payments, Mastercard

- The Mastercard approach to threat forecasting
- How threatcasting works – an in-depth look
- An insight of recent threatcasts

11:50 **An inside look at the attack lifecycle**

Jason Steer, Principal Security Strategist, Recorded Future

- Learn how to monitor and alert on unusual or potentially malicious activity inside your organisation
- Specifically understand how credentials for your users can be stolen and sold
- Specifically understand how Initial Access Broker posts can be reviewed to protect your organisation
- Discover how using threat intelligence can provide insights to help your organisation detect potential events before they cause serious business impact

Agenda | Day 2 | 3rd March 2022

12:10 DORA: Your framework for smart thinking

Dr Rois Ni Thuama, Head of Cyber Governance, Red Sift

During this session, Rois will explore:

- Why you should listen to the FBI's warnings
- Promoting smarter thinking with DORA
- How DORA will reduce business disruption
- The cost of doing nothing… from civil litigation and fines to criminal penalties

12:30 EXECUTIVE PANEL DISCUSSION Future-proofing the CISO

Helen Rabe, CISO, Abcam; **David Whitelegg,** European Security Officer, Compass Group; **Zibby Kwecka,** Head of Information Security, Heineken UK; **Jon Townsend,** CIO, National Trust; **Simon Goldsmith,** Director for Information Security, OVO Energy

- How has the evolution of the threatscape and security technology affected the role of the CISO in the last five years?
- What are the most important skills and qualities CISOs will need to possess over the next five years?
- How must the organisation and staffing of cybersecurity teams change? (bigger, smaller, skillsets, diversity?)

12:50 Education Seminars | Session 5

BeyondTrust	**The seven perils of privilege** **Brian Chappell,** Chief Security Strategist (CSS), EMEIA & APAC, BeyondTrust
FireMon	**Improving security outcomes and eliminating security headaches through a threat-led approach** **Bryan Littlefair,** CISO & Cybersecurity Consultant, presenting on behalf of FireMon
Illumio	**How isolation stops the spread of ransomware** **Trevor Dearing,** Director of Critical Infrastructure Solutions, Illumio
Menlo Security	**The next class of browser-based attacks** **Brett Raybould,** Head of Solutions (EMEA), Menlo Security
Proofpoint	**Ransomware: One of your biggest risks – don't let it in** **Alistair Mills,** Director, Sales Engineering, Northern Europe, Proofpoint

13:30 Lunch and networking break

14:30 EXECUTIVE PANEL DISCUSSION Securing financial services

Crawford Thomas, Global Head of Cyber Threat Intelligence, Credit Suisse; **Ruth Anderson,** Director Group Operational Resilience and Security, Lloyds Banking Group; **Jill Robertson,** Head of Information Security Change Team, Metro Bank

- How do new resilience regulations help in the battle against cybercriminals?
- Does cybersecurity fit naturally into the three lines of defence model?
- Third-party dependency: do we need to talk about Cloud oligopoly?
- How can we collaborate when regulators and legislators make it so hard?

14:50 Supply chain cybersecurity: Reduce your risk

Chris Waynforth, Area VP, EMEA North, Imperva

Why supply chain attacks affect every business and protecting against them is everyone's business – not just security. Hear

- How to minimise the software supply chain risk, without business impact
- How to protect the application layer – a key attack vector
- What new technologies exist to defend against this critical risk

15:10 Why your MFA will not keep the bad guys out

Chris Robins, Senior Sales Engineer, EMEA, Beyond Identity

- MFA requirements have changed
- Cybercriminals have become more sophisticated in their attacks, and traditional MFA that relies on passwords and other weak factors can't keep up
- Remote working has expanded and rapid cloud adoption demands that companies ensure the identity of the user behind every device, and assess the level of risk before access
- Unlike traditional MFA, Beyond Identity can protect your data from advanced attacks
- Traditional MFA relies on weak factors like passwords and one-time codes. Beyond Identity eliminates passwords and only uses strong factors like asymmetric cryptography and biometrics to protect your organisation from phishing, ransomware attacks, and other password-based attacks

15:30 Networking and refreshments

15:50 The FBI's overseas posture

Eric Smithmier, Assistant Legal Attaché, FBI London, Cyber Division, & **Jensen Penalosa,** Assistant Legal Attaché, FBI

- Coordination with UKIC partners
- Public/private sector engagement
- Cyber-threat intelligence sharing

16:10 Cybersecurity, achieving security convergence in interesting times

Ian Shaw, Head of Risk and Security, South East Coast Ambulance Service, NHS Foundation Trust

- The challenge of truly integrating security and creating a converged solution
- The human component within cybersecurity, why EQ is as critical as IQ
- Early observations on how COVID has skewed risk perception

16:30 Chairman's closing remarks and Congress close

Education Seminars	
Beyond Identity **Beyond Identity's passwordless MFA: The only way to positively verify user identity at login** **Chris Robins,** Senior Sales Engineer, EMEA, Beyond Identity	MFA requirements have changed. Cybercriminals have become more sophisticated in their attacks, and traditional MFA that relies on passwords and other weak factors can't keep up. Remote working has expanded and rapid cloud adoption demands that companies ensure the identity of the user behind every device, and assess the level of risk before access. Traditional MFA relies on weak factors like passwords and one-time codes, Beyond Identity eliminates passwords and only uses strong factors like asymmetric cryptography and biometrics to protect your organisation from phishing, ransomware attacks, and other password-based attacks. In this seminar you'll learn how to: • Stop unknown users and devices from authenticating – block malevolent access attempt • Enforce and prove compliance – force adherence to regulations • Simplify roll out, empower your users – deploys within minutes, allows users to self enroll • Remove productivity killers – no need to locate a 2nd device, fish out a code or link • Reduce cost – no more forgotten password lock outs!
Devo **Single source of truth – the fundamental building blocks for an effective security operations centre** **Nipun Gupta,** Cybersecurity Specialist, Devo Inc.	How effective is your security operations and your ability to gather evidence, investigate and find source data? If unsure, you're not alone. Combating today's threats requires new approaches to how your SOC manages its data, analytics, and expertise. Join Devo as we explore innovative ways your security team can thrive in the era of massive data growth, talent shortage, and constantly evolving threats. • Cloud-based solutions scale to achieve the critical full visibility into threats, giving you a single source of truth • Analytics that use automation and machine learning uplift analysts' performance, saving your security team valuable time • Community expertise augments your tribal knowledge to quickly resolve threats, helping you bridge the industry talent gap
Imperva **APIs as your ultimate honeypot** **Pal Balint,** Senior Sales Engineer, Imperva	How the use of the accelerator of all modern web applications goes horribly wrong, and what to do to prevent it. • What are some of the popular API security measures and why they are not enough? • How to recognise data leakages and what to do to counter them • How to spot irregular behaviour in both B2B and B2C APIs
Netacea **BLADE: Cutting through the complexity of business logic attacks** **Matthew Gracey-McMinn,** Head of Threat Research, Netacea, & **Cyril Noel-Tagoe,** Cyber Threat Evangelist, Netacea	The bot attack landscape is growing in maturity, and as it does it's crucial that bot management vendors develop and implement sophisticated bot defence systems to combat the growing threat. To facilitate this next phase of bot defence, we have developed a bot management framework, built with the combined input of vendors and influencers throughout the industry. • Taking inspiration from the MITRE ATT&CK Framework, the Business Logic Attack Definition (BLADE) Framework captures all automated bot threats and their life cycle in a series of comprehensive kill chains • The BLADE Framework enables all bot vendors to take a proactive approach to tackling the malicious bot threat, with a greater shared understanding and knowledge that ultimately empowers businesses • During this Educational Seminar, we will introduce the BLADE Framework, discussing how it captures automated bot threats using a series of kill chains, and how a bot framework will help businesses fight sophisticated bots and protect customers from automated threats • We will draw upon use cases where other organisations have successfully employed the framework

Education Seminars	
Recorded Future **The business of fraud: Sales of PII and PHI** **Lewis Brand,** Senior Sales Engineer, Recorded Future	• Gain knowledge on how personally identifiable information (PII) and patient health information (PHI) are highly sought after data across criminal sources, both on the clearnet and dark web • Learn how our research identified that threat actors use various attack vectors, including social engineering and infostealer malware variants, to obtain victim PII or PHI • Understand how, once this data has been harvested, threat actors monetise it through traditional cybercriminal sources (dark web, including forums, marketplaces, and shops) and messaging platforms • Discover how threat actors interested in buying and selling PII and PHI data continue to improve their tactics, techniques, and procedures (TTPs), with vendors selling customised services and methods that include access to accounts with sensitive user data, methods to defeat security measures, and counterfeit documentation
Red Sift **Why building a people-first security culture is the key to cyber-defence in 2022** **Engin Yilmaz,** Product Director, Red Sift	2022 looks set to be another year where organisations will face an onslaught of cyber-attacks. With phishing attacks still the number one cause of security breaches, and 85% involving the human element, businesses need clear, concrete advice on how to act. • The importance of building a people-first cybersecurity culture • Why phishing awareness training and Secure Email Gateways aren't enough • How new 'in the moment' threat intelligence products can help to mitigate human error
SenseOn **Root cause analysis in moments, not days** **Brad Freeman,** Director of Technology, SenseOn	Identifying the root cause of security events quickly and accurately is a critical success factor for security operations. By not relying on true root cause analysis, we hold significant compound risk every time we are 'almost certain' that an event was benign. This education seminar discusses key operational problems with strategic impact in existing security operations teams including how they can be measured, how this can be used as a basis for threat hunting, and how it can help with SOC efficiency improvements. In this session you will: • Understand why root cause analysis is important for process improvement and risk reduction. • Consider new metrics and different methods of measuring SOC efficiency beyond existing detection and response metrics such as MTTR & MTTD. • Apply root cause analysis as the basis of threat hunts across complex networks and as a driver for security improvements
ManageEngine **How to use the MITRE ATT&CK framework to stop ransomware** **Ram Vaidyanathan,** Cyber Risk and Security Expert, ManageEngine	With the MITRE ATT&CK framework, you can understand the modus operandi of potential attackers. But how exactly can you use this framework to stop ransomware? A typical ransomware attack has five stages: Initial exploitation, installation, backup destruction, encryption, and extortion. In this talk, I will try to map each of these stages to the different tactics and techniques identified in the MITRE ATT&CK. The objective is to understand the intricacies of ransomware so that you can defend against it effectively. Key learnings: • Tactics, techniques and procedures covered in the MITRE ATT&CK framework • What makes ransomware such a big threat for organisations? • Mapping the 5 stages of ransomware to the MITRE ATT&CK • Tips for effective defence

Education Seminars	
Okta **How identity can accelerate digital trust** **Ian Lowe,** Director of Solutions Marketing, EMEA, Okta	In today's digital-first world, customers and citizens are being asked to share their data in new ways and for new purposes. While most are increasingly comfortable interacting online they expect secure, consistent services in return for their valuable personal information. Seamless digital experiences are critical to securing our trust – and this starts with identity In this session we will look at: • What are the top drivers of trust online? • Whether digital IDs are winning acceptance • Who's responsible for protecting personal digital identity
Picus Security **The CISO's challenge – how to be more proactive with less** **Tim Ager,** VP of Sales, EMEA, Picus Security	In cybersecurity, being proactive is often easier said than done. With so much to do to manage your organisation's security posture day-to-day, it can be almost impossible to find the time to stay on top of the latest threat intelligence and apply it to improve your defence. Join Tim Ager, VP at Picus Security, to learn how Breach and Attack Simulation (BAS) technology is helping CISOs to address this very challenge by automatically validating the effectiveness of security controls and by reducing the strain on security operations. Learn how BAS is helping security teams to: • Validate preparedness against the latest threats • Swiftly address prevention and detection gaps • Measure and benchmark threat coverage and visibility • Rationalise investments to improve efficiency and value • Demonstrate assurance to the boardroom
Synack **Hacking for the greater good: Using hackers to beat hackers** **Justin Shaw-Gray,** Sales Director for UKI and South Africa, Synack Inc, & **Mark Walmsley,** Chief Information Security Officer (CISO), Freshfields Bruckhaus Deringer LLP	For CISOs, designing security for a decentralised workforce requires revisiting where and how security and risk management leaders direct their efforts. In this session, Synack's Justin Shaw-Gray and Mark Walmsley, CISO, Freshfields Bruckhaus Deringer LLP. will discuss the security challenges CISOs are facing in today's business climate and how Synack's innovative crowdsourced security model and continuous pen testing offering address these challenges. Attendees will learn • How concerns and security implications for organisations and their remote workforce have played a role in security decisions • How to secure your organisation while managing a remote workforce from the executive's perspective • How agile businesses are able to respond quickly to opportunities or threats • How security researchers are playing a pivotal role in securing company's assets
Tessian **Master defence in depth: Supercharging the security of your Microsoft email environment** **Neil McRae,** Solution Engineer, Tessian	• Hear about the benefits of joining forces between machine learning and threat intel to bring you closer to becoming a master of defence in depth! • We will discuss how to build high impact defence augmenting Microsoft with behavioural technologies • How threat attackers are actively deploying new BEC, ransomware, and ATO attacks to target enterprise companies • How to own the best practices of multi-layered security to fulfil the security requirements of cloud API architecture

Education Seminars	
Vectra **How AI-based 'Threat Detection & Response' finds and stops ransomware** **Steve Cottrell,** EMEA CTO, Vectra	Cybercriminals are always looking for easy targets and opportunities to steal personal information. With no application, network, or data centre being invulnerable, decision-makers often harbour a false sense of security about their ability to fend off hackers – especially when they're not armed with the necessary tools to succeed. During our presentation we will cover: • How prepared your organisation is to detect and respond to a ransomware attack • What approaches other organisations are taking to stop ransomware gangs • How to detect and respond to Ransomware before it impacts you
CrowdStrike **How to reveal secrets from criminal forums and interrupt adversaries in their tracks** **James Burchell,** Senior Security Engineer, CrowdStrike	A thriving e-Crime ecosystem of services, distribution, and monetisation makes it easy for malicious operators to 'set up shop', join the cybercrime scene, and target victims. In this session, we will focus on one specific use case of monitoring access brokers, following the bread crumbs they leave behind, and identifying critical threat activity in a high-noise, fast-moving criminal ecosystem. • Understand threat actor operations and value chains of specialised services • Identify and interpret the bread crumbs operators leave behind when selling illegitimate merchandise • Refine high noise and difficult to access environments to actionable insights • Learn steps to form a monitoring strategy that follow the bread crumbs
CybelAngel **Finding the leaky data links in your supply chains – data security beyond perimeters** **Vijay Kishnani,** Lead Cyber Security Engineer, CybelAngel	Ask yourself, where is the risk in sharing data with third parties? Is the risk the third party, or is the risk having your data leak? The real danger is the data leak! The leak being at a third party just makes it more challenging to locate. Instead of making third parties jump through long and sometimes unproductive audits, a new perspective is needed – a data risk first approach. A data risk first approach focuses on locating whatever data matches your organisation's regardless of where it appears. By focusing on which data matches, you gain visibility and protection far beyond a company's perimeter into third, fourth, and fifth parties. This increase in visibility frees cybersecurity teams from choosing which partners get monitoring. You will learn: • Why your risk is with the data, not third parties • What is a data risk first approach? • How DRPS tools can assist in a data risk first approach
HelpSystems **HelpSystems Data Security Suite: Protecting you data with layered security solutions** **Nick Hogg,** Director of Technical Training, HelpSystems	Today's organisations have to protect their data from a host of external threats and internal risks. Using a layered approach to our data security still makes a huge amount of sense, even as we move more of our data to the cloud. By using different detection and mitigation techniques, we provide resilience for those instances when a system or manual process becomes compromised, because you have other systems there to catch and prevent the breach. This session will cover: • The data security challenges that organisations face • How people, processes and technology can be used in order to protect data throughout its entire lifecycle • How the HelpSystems Data Security Suite can assist with protecting your sensitive data • How organisations can regain control of their data by identifying and classifying sensitive data • Attend this session for inspiration and ideas on how to more effectively protect your data and get the most out of your data security investments

Education Seminars	
Kenna Security **Cisco SecureX + Kenna Security: Radical simplification in the new era of cybersecurity** **Stephen Roostan,** VP, EMEA, Kenna Security	Cybersecurity is a complex challenge. What's needed is a way to radically simplify security operations to be simple, automated, and democratised. So, no matter the complexity of your IT environment, and how many threats may be targeting your organisation, protecting it shouldn't be difficult. Cisco recognises this need and is defining a path forward. By integrating Kenna Security's acclaimed risk-based vulnerability management platform, Cisco's SecureX will help organisations solve a notoriously difficult piece of the security puzzle to accelerate response time for cyber-readiness. In this session, Stephen Roostan, Vice President for EMEA at Kenna Security, now part of Cisco, details why Cisco's acquisition of Kenna is a pivotal move for customers and the industry as a whole. • Real-world threat intel, machine learning, and predictive analytics help teams identify and prioritise their riskiest vulnerabilities • Remediation teams will know what to patch and when, saving time, money, and resources • Integrating enterprise security management solutions into one centralised location breaks down silos and extends detection and response capabilities • Automated workflows help lower organisational risk profiles, improve collaboration between Security and IT, and shrink their attack surfaces • Kenna Risk Scores help stakeholders clearly assess the relative risk of a specific vulnerability, asset class, workgroup, or organisation as a whole • To speed decision making with prioritisation of vulnerability data based on threat intelligence and asset business value • Adding Kenna Security to SecureX extends the broadest XDR capabilities in the industry
OPSWAT **File upload protection: A critical gap in web app security** **Adam Gurney,** Sales Engineer, OPSWAT	Digital transformation is a must for today's organisations, resulting in a migration from paper-based to digital documents. Millions of documents are now being shared among collaborators weekly and monthly – uploaded to either a web portal, customer portal (insurance or mortgage applications) or support portal (attaching files to your support ticket). At the same time, an enormous amount of effort is invested into building high-availability, fault-tolerant systems and securing them. However, file upload remains a major attack vector and far too often is not covered by traditional web application defences. In this seminar, Adam Gurney, Sales Engineer at OPSWAT will cover three types of risks to web applications and how to apply a Zero Trust model to both users and the files they upload and the devices from which these uploaded files originate. Risks from: • Threat actors who submit malicious files to gain access to the organisation's IT infrastructure • User who submits sensitive data in violation of an application's terms of service • Inadvertent hosting and distributing malicious files uploaded by a threat actor

Education Seminars	
4Data Solutions **Observability; a data driven approach to cloud security** **Ian Tinney,** CEO, 4Data Solutions	Securing cloud data is a sizable challenge. Doing it properly means processing huge amounts of data – which, given the associated cost, can become unviable. Being smart with your data by being able to source, reduce, shape, enrich and route it with complete flexibility and agility enables you to overcome this problem and make full data security viable for your organisation. We explore this security challenge in more detail looking at: • Building an inventory • Recording the state • Monitoring for change • Securing user accounts • Curating data • Observing And what technologies will help deliver all of this. What you will learn: • Dealing with the 'analysis versus privacy' dilemma • Cloud adoption drivers; the electric car of the data world (doing it for the greater good) • Securing data – the need for flexibility, prioritisation and protection • Borrowing from APM – taking an observability approach to security data • Data use cases – different storage for different data needs • Organisational security – insights into a data driven approach to cybersecurity
Cequence Security **Frictionless API security strategies** **James Sherlow,** Systems Engineering Manager, EMEA, Cequence Security	Organisations are rapidly adopting an API-first development strategy and methodology because of the power, flexibility and efficiency that APIs provide. The shopping, finance, manufacturing or marketing apps we use every day are all based on APIs, connecting back to compute resources located elsewhere – be it the cloud, the data centre or both. Critically, threat actors leverage APIs for the exact same reasons that developers do. APIs are susceptible to a range of automated attacks and vulnerability exploits that can lead to data loss and system compromise. To protect existing and future APIs, organisations need to implement forward-looking API security strategies that are frictionless and transparent to the development team. This session will delve into the different approaches to protecting APIs from various security risks and how security teams can make strategic decisions on the depth of protection deployed. • Discover: Complete visibility of public-facing APIs, their location & service categories • Detect: Identification of sophisticated API attacks targeting apps & data • Defend: Ability to respond in real-time & block attacks
Cofense **Adaptive email security architecture: Moving from incident response to continuous response** **Alain Salesse,** Senior Sales Engineer, Cofense	With so much focus on cyber-attack prevention, many security teams have adopted an incident response mindset versus one that assumes systems are compromised and require continuous monitoring and remediation. Join us for this informative session that walks through the benefits of implementing an adaptive security architecture and risk framework, and how to classify your existing and potential email security investments to increase your security posture while reducing costs, vendors, and configuration complexity. This session will cover: • What is adaptive security architecture • Objectives of adaptive security architecture • Risk framework • The current situation in email and phishing security • Implementing adaptive security architecture and risk framework with Cofense

Education Seminars	
Cybersixgill **Chihuahuas VS. muffins: Developing AI solutions for threat intelligence problems** **Benjamin Preminger,** Product Manager, Cybersixgill	AI and automation are well-known industry buzzwords, but how can they actually benefit modern threat intelligence practices and capabilities? In this interactive workshop we will quickly run through high-level concepts in AI/ML and automation, and then deep-dive into some of the practical challenges and opportunities AI offers to combat cyber-threats. Leveraging the speaker's real-world experience of developing home-grown AI solutions, the workshop will strive to answer key questions such as: • How can organisations prioritise work on AI initiatives? • What challenges can I expect in developing AI? • Is it worth it?
Darktrace **Fast and furious attacks: Using AI to surgically respond** **Toby Lewis,** Head of Threat Analysis, Darktrace	Fast-moving cyber-attacks like ransomware can strike at any time, and security teams are often unable to react quickly enough. Join Toby Lewis, Head of Threat Analysis at Darktrace, to learn how Autonomous Response uses Self-Learning AI's understanding of 'self' to take targeted action to stop in-progress attacks, without disrupting your business. • Learn how Autonomous Response knows exactly the right action to take, at the right time, to contain an in-person attack • How AI takes precise action to neutralise threats on the behalf of security teams • Use of real-world threat finds to illustrate the workings of Autonomous Response technology
Intel 471 **Back to the future** **Maurits Lucas,** Director of Product Marketing, Intel 471	Those who do not learn from history are doomed to repeat it, the saying goes. On this, the 20th edition of the e-Crime Congress, join us in this session as we look at the lessons from the past to predict the near future. From the first case of nation-state hacking – which happened earlier than you may think – to the rise of financially motivated cybercrime and the ecosystem of products, services and goods that arose to facilitate it, we'll plot the trends and use them to predict the future. From banking botnets to WhatsApp fraud, Ransomware-as-a-Service, cryptocurrencies and the blurring lines between nation-state and cybercriminals to IoT and everything as a service: the future is already here! How about our understanding of its threats? Key takeaways: • How far we've come from humble beginnings both in the type of attacks but also in the tooling we have at our disposal • First, there were nation-state actors and cybercriminals — now the two are mixing and blurring that it is hard to tell which is which anymore. Sometimes they don't even seem to know themselves! • The impacts of attacks are increasing, but at the same time over the past 6 months, some new ground rules have started to emerge • What future trends we can distil from recent events. No matter what happens, fundamental changes have occurred that come with consequences
BeyondTrust **The seven perils of privilege** **Brian Chappell,** Chief Security Strategist (CSS), EMEIA & APAC, BeyondTrust	Cybercriminals are opportunistic and merciless. They will target security vulnerabilities such as weak passwords or unnecessary administrator rights. The National Cyber Security Centre recently found that 23.2 million victim accounts worldwide used 123456 as the password, and many companies still provide full admin rights to employees, despite the widely known risks involved. In this session, we will cover the 'Seven perils of privilege' – addressing what they are, their causes, the effects of leaving them unaddressed, and (most importantly) solutions. Join us to learn: • What the seven perils of privilege are and why they matter • Why poor password practices, lax cloud security (and much more) create risk • How to mitigate these risks and protect your organisation

Education Seminars	
FireMon **Improving security outcomes and eliminating security headaches through a threat-led approach** **Bryan Littlefair,** CISO & Cybersecurity Consultant, presenting on behalf of FireMon	The world has changed. And so has the threat landscape. Organisations are facing a landscape of scarce security resources, increased pressure from regulators, and an unprecedented volume of threats. And the reality is, we can no longer rely on the 'old way' of managing security. Change brings challenges, and this is being felt from the boardroom down. For organisations to improve security outcomes, they need to improve security operations, and that starts with a threat-led approach. Join us as we explore: • The global threat of change: The real-life impacts to businesses right now • A threat-led approach: Best practices in how to improve your security operations and improve your security outcomes • Avoid violations. Avoid risk. Avoid fines. How to get a real handle on your risk profile by adopting a threat-led approach to security
Illumio **How isolation stops the spread of ransomware** **Trevor Dearing,** Director of Critical Infrastructure Solutions, Illumio	• See how to stop the propagation of ransomware • Identify the potential weaknesses in your infrastructure • Build a more resilient defence against future threats
Menlo Security **The next class of browser-based attacks** **Brett Raybould,** Head of Solutions (EMEA), 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
Proofpoint **Ransomware: One of your biggest risks – don't let it in** **Alistair Mills,** Director, Sales Engineering, Northern Europe, Proofpoint	Mitigating the risk of ransomware to your business has become the job of every security product and service available today. But measuring the impact of technology on the risk of exposure is rarely achievable until it's too late. Endpoint security and EDR solutions will help you respond once you already have a ransomware problem. So how do you measurably reduce the risk of the problem occurring before it's too late? • What are the common attack vectors for ransomware? • How you can quickly reduce your risk