Post event report

Strategic Sponsors

BeyondTrust
DARKTRACE
Forcepoint
MENLO SECURITY
Orange Cyberdefense
proofpoint.
SEARCHLIGHT Security

Education Seminar Sponsors

Abnormal
ARMIS.
AXONIUS
CWSI.
e2e assure
HUNTERS
GATEWATCHER
imperva
INTIGRIT
Malwarebytes
netwrix
OBSIDIAN
ONE IDENTITY by Quest
RED SIFT
SentinelOne
SOCRadar®
virtru

Branding Sponsors

THALES
YogOsha

“ e-Crime Congress is one of the events in my ‘must attend’ list. I always find it informative. It also offers networking opportunities to learn what the peers in the industry are doing in an ever-changing threat landscape. ”

IT Security & Risk Officer, UBS

“ The summit was really valuable, as always. There was a good mix of peer, vendor and expert sessions, the breakouts were not too pushy and the content was good overall. The sessions were short and snappy, there was little contention for me in terms of which breakouts I attended and could (and did) follow up with the vendors I missed outside of the sessions. The organisation, up to having desks rather than just rows of chairs, was very good. ”

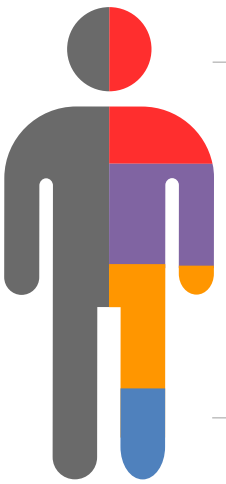
Head of Information Security, Salary Finance

Inside this report:

Key themes

- From cybercrime to cyberwar
- From smart machines to smart cities – securing the IoT
- The perimeter is dead – that is not just hype
- Securing digital currencies
- Getting real about automation, AI and the rest
- Keeping citizens safe
- All aboard the Cloud
- Developing the next generation of security leaders
- The rise and rise of effective cybersecurity regulation
- Securing the technologies of the future
- Reining in BigTech
- 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

Bev Allen, CISA, Quilter

Simon Brady, Managing Editor, AKJ Associates

Adrian Clark, Data Security Specialist, Imperva

Carl Curran, VP EMEA, Axonius

Emmanuel Dahunsi, Security Architect EMEA, Goldman Sachs

Hanah Darley, Head of Threat Research, Darktrace

Ian Dutton, Senior Sales Engineer, GateWatcher

Nick Edwards, VP Product Strategy, Menlo Security

Chris Fuller, Principal Product and Solutions Architect, Obsidian Security

Simon Goldsmith, Director for Information Security, OVO Energy

Joshua Harris, Senior Customer Success Engineer, Red Sift

Ash Hunt, CISO, Sanne Group

Glen Hymers, Head of Data Privacy and Compliance, Cabinet Office

Federico Iaschi, Resilience Engineering Partner Change – Digital Security Department, Virgin Media O2

Khalid Khan, Sales Engineering Director (NEUR), Forcepoint

Nicholas King, CISSP Principal Solutions Consultant, Orange Cyberdefense

Sarah Lawson, CISO, UCL

Hanan Levin, VP Sales EMEA, Hunters

David Lomax, Systems Engineer, Abnormal Security

James Maude, Lead Cyber Security Researcher, BeyondTrust

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

Anthony Moillic, EMEA Field CISO, Netwrix

PJ Norris, Senior Security Engineer, SentinelOne

Dr Gareth Owenson, CTO, Searchlight Security

David Palmer, Business Lead for Blockchain Technology, Vodafone

Samet Sazak, Technical Account Manager, SOCRadar

Stuart Sharp, Vice President of Solution Engineering, One Identity

Derek Skinner, Global Manager, Investigations, Absolute on behalf of CWSI

John Skipper, CISO, Metro Bank

Anthony Smyth, Senior Director, Solution Architects EMEA, Armis

Scott Storey, Digital Information & Cyber Security Lead, Parkdean Resorts

Danielle Sudai, Cloud Security Operations Lead, Deliveroo

Carl Urban, Lead Cyber Consultant, e2e-assure

Llewellyn Wells, Solutions Consultant, Virtru

Lee Whatford, CISO, Domino's Pizza

Mark Wiley, Senior Account Executive, Intigriti

Kenny Williams, Solution Engineer, Malwarebytes

Agenda

08:00 Registration & networking

08:50 Chairman's welcome

09:00 **What good 'Cybersecurity' looks like' to different stakeholders**

Simon Goldsmith, Director for Information Security, OVO Energy
- What does the Board mean? What does the CISO mean?
- What do the frontline security analysts, incident responders etc think?
- And how do you blend all these different perspectives into a coherent cybersecurity framework?

09:20 **Breaking the ransomware attack chain**

James Maude, Lead Cyber Security Researcher, BeyondTrust

Join BeyondTrust and learn the how you can break the attack chain and establish a solid foundation for ransomware project success.
- Common ransomware attack chain entry points
- Practical steps you can take to block entry
- How PAM ensures ransomware project success

09:40 **Using the dark web to gather pre-attack intelligence**

Dr Gareth Owenson, CTO, Searchlight Security
- Defining the pre-attack stage of a cyber-attack
- How intelligence on the pre-attack tactics of threat groups can help organisations preempt and prevent attacks
- Real life examples of when threat groups' pre-attack reconnaissance and resource development activity could be observed in the dark web
- How dark web intelligence can be mapped to pre-attack tactics of the MITRE ATT&CK framework to practically improve defences

10:00 **Fireside chat: A CISO's perspective on….**

Simon Brady, Managing Editor, AKJ Associates, and **John Skipper,** CISO, Metro Bank
- How the macroeconomic downturn will affect CISOs, budgets and security
- Dealing with the risks of state-sponsored cyber-attacks and spillovers
- Practical tips for implementing a risk-based approach to cybersecurity

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

Abnormal Security	GATEWATCHER	Imperva	Intigriti	Obsidian Security	SentinelOne
Key considerations for choosing the right cloud email security platform	**Understand the technologies required for the effective and efficient detection of cyber-threats to protect your organisation**	**Demystifying data protection: Steps to find, monitor and control without chaos**	**An introduction to bug bounty programs for businesses**	**Cookies and Spam: Exploring MFA bypass techniques used by attackers to breach SaaS applications**	**Debunking common myths about XDR**
David Lomax, Systems Engineer, Abnormal Security	**Ian Dutton,** Senior Sales Engineer, GATEWATCHER	**Adrian Clark,** Data Security Specialist, Imperva	**Mark Wiley,** Senior Account Executive, Intigriti	**Chris Fuller,** Principal Product and Solutions Architect, Obsidian Security	**PJ Norris,** Senior Security Engineer, SentinelOne

11:00 Networking break

11:30 **SENIOR LEADERSHIP PANEL** **Security technology**

Danielle Sudai, Cloud Security Operations Lead, Deliveroo; **Ash Hunt,** CISO, Sanne Group; **Sarah Lawson,** CISO, UCL; **Federico Iaschi,** Resilience Engineering Partner Change – Digital Security Department, Virgin Media O2
- Different approaches to selecting and consolidating security technologies
- Budget and investment questions as more vendors broaden their capabilities
- Replacing legacy cybersecurity technology
- One-stop shop versus security stack
- Building a continuous control environment for cybersecurity

11:50 **Data doesn't lose itself. People lose data; It's time to change the way we protect it**

Alistair Mills, Director, Sales Engineering, Northern Europe, Proofpoint
- Insider risk and data loss prevention are a top concern for organisations today. And it makes sense, with a distributed workforce and increasing reliance on technology, legacy, on-prem DLP technology hasn't lived up to its promises
- Data loss begins with people, whether negligent, compromised or malicious insiders. So, how do you better protect your organisation?
- In this session, you'll gain insight into the importance of understanding user risk profiles, how to better understand and respond to people-led data breaches and real-world examples and best practices to improve your data and user security

12:10 **How AI can think like an attacker**

Hanah Darley, Head of Threat Research, Darktrace
- In the face of skyrocketing cyber-risk, detecting and responding to attacks is no longer enough. Organisations must take proactive steps to prevent threats before they happen, and to recover if compromised
- In this session, Darktrace unveil an ambitious new approach to security, with core engines powering AI technologies to prevent, detect, respond, and ultimately heal from attacks
- Together, these engines combine to strengthen organisations' security posture in a virtuous AI feedback 'loop,' which provides powerful end-to-end, bespoke, and self-learning solutions unique to each organisation

Agenda

12:30 **Your network security stack is failing you: Learn how ransomware bypasses secure web gateways**

Nick Edwards, VP Product Strategy, Menlo Security

- With one third of organisations experiencing ransomware attacks at least weekly, and 9% doing so more than once a day – why are current attacks different?
- How is ransomware bypassing network security detection from traditional security tools such as Secure Web Gateways, sandbox analysis and phishing detection solutions?
- Reacting to the increased attack surface of hybrid work and cloud apps, what are the different approaches organisations are successfully deploying to mitigate the threat of ransomware?

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

Axonius	CWSI	e2e-assure	Hunters	Netwrix	Virtru
From asset management to asset intelligence: Crossing the CAASM **Carl Curran,** VP EMEA, Axonius	**Tales from the frontline** **Derek Skinner,** Global Manager, Investigations, Absolute on behalf of CWSI	**Elevating cybersecurity as a business enabler and source of competitive advantage** **Carl Urban,** Lead Cyber Consultant, e2e-assure	**Hunters: The SOC of the future** **Hanan Levin,** VP Sales EMEA, Hunters	**Streamlining compliance with zero standing privilege** **Anthony Moillic,** EMEA Field CISO, Netwrix	**Embrace a new kind of security: Zero Trust Data Control** **Llewellyn Wells,** Solutions Consultant, Virtru

13:30 Lunch break

14:30 **The metaverse opportunity**

David Palmer, Business Lead for Blockchain Technology, Vodafone

- What are the key enablers for virtual and real worlds to co-exist
- The key challenges
- Security, identity, jurisdiction, copyright and ownership

14:50 **Data breach incident response – the rest of the iceberg**

Nicholas King, CISSP Principal Solutions Consultant, Orange Cyberdefense

An alternative view on the preparation stage of incident response. How these activities not only help you to respond to an incident but in many ways can reduce the risk of the incident happening in the first place. During this presentation we will explore:

- Data discovery and classification
- The principle of least privilege
- Data life-cycle management
- Threat detection

15:10 **Simplifying security and reducing risk with SASE & Zero Trust**

Khalid Khan, Sales Engineering Director (NEUR), Forcepoint

- What's the best approach in a hybrid world?
- How does SASE & Zero Trust Architecture help prevent cyber-incidents?
- How do you show and verify positive value from a security platform?

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

Armis	Malwarebytes	One Identity	Red Sift	SOCRadar
Why asset visibility is a critical foundation of operational and cyber-resilience **Anthony Smyth,** Senior Director, Solution Architects EMEA, Armis	**Threat disruption: Securing 2022 from 2021** **Kenny Williams,** Solution Engineer, Malwarebytes	**A unified defence against identity sprawl threats** **Stuart Sharp,** Vice President of Solution Engineering, One Identity	**Email security & brand protection: Two sides of the same coin?** **Joshua Harris,** Senior Customer Success Engineer, Red Sift	**How to track your data on the dark web** **Samet Sazak,** Technical Account Manager, SOCRadar

16:10 Networking break

16:30 **A CISO's guide to multi/poly cloud security**

Emmanuel Dahunsi, Security Architect EMEA, Goldman Sachs

- What is multi/poly cloud and what benefits do they provide?
- What are the security challenges of multi/poly cloud?
- Security strategy for multi/poly cloud

16:50 **SENIOR LEADERSHIP PANEL** **Security challenges**

Glen Hymers, Head of Data Privacy and Compliance, Cabinet Office; **Lee Whatford,** CISO, Domino's Pizza; **Scott Storey,** Digital Information & Cyber Security Lead, Parkdean Resorts; **Bev Allen,** CISA, Quilter; **Simon Goldsmith,** Director for Information Security, OVO Energy

- Asset inventories (devices, applications, identity, network, data)
- Overall technology landscape complexity
- 'Digital' transformations of the business/products
- Testing and measuring the effectiveness of the cybersecurity control environment
- Incident response and problem management
- Ensuring the same coverage/visibility over cloud environments as on-prem
- Managing supply chain risk in a world less tolerant to long delays around supplier assurance (post covid)
- Web 3.0 and the next generation of the internet: securing new technologies and services which are inherently decentralised

17:30 Drinks reception

18:30 Conference close

Education Seminars	
Abnormal Security **Key considerations for choosing the right cloud email security platform** **David Lomax,** Systems Engineer, Abnormal Security	Email is both a necessary communication medium, and the most vulnerable area for an attack. Year after year, adversaries find success in abusing email to gain a foothold into an organisation – deploying malware, leaking valuable data, or stealing millions of dollars. Unfortunately, email threats are only growing in number. Business email compromise accounts for 35% of all losses to cybercrime, and the Verizon Data Breach Investigations Report holds that phishing remains the top entry point for breaches – a position it has held for years. Does that mean email is doomed, and we should give up? Quite the opposite. But the shift to cloud email requires one major thing – a shift to cloud email security. Attend the Abnormal Security session for answers to your most pressing questions, including: • What are modern email threats, and how are they different from legacy attacks? • Which email threats are most concerning, and how can we defend against them in the cloud environment? • Which technical capabilities are required when protecting cloud email? • How can cloud email security platforms detect the most dangerous attacks?
Armis **Why asset visibility is a critical foundation of operational and cyber-resilience** **Anthony Smyth,** Senior Director, Solution Architects EMEA, Armis	Having complete and continually up to date visibility into your connected devices, is the platform on which to assess and build your cybersecurity posture. Which can include: • Ensure compliance with security standards and regulation • Optimise the security tools within your environment • Ability to prioritise vulnerability management
Axonius **From asset management to asset intelligence: Crossing the CAASM** **Carl Curran,** VP EMEA, Axonius	As the sprawl of devices, device types, and solutions continues to skyrocket, environments only grow more complex. But there's good news: asset management has evolved. Today's 'asset intelligence' moves from a spreadsheet approach to an API-driven, always up-to-date view into all assets via integrations of existing tools, data correlation at scale, and querying capabilities to find and respond to gaps. Join this session to learn how asset intelligence and the emerging Cyber Asset Attack Surface Management (CAASM) category: • improves security hygiene • reduces manual work • remediates gaps
CWSI **Tales from the frontline** **Derek Skinner,** Global Manager, Investigations, Absolute on behalf of CWSI	• How to enable the modern frontline policing • Securing and managing the mobile fleet – who are still the weakest links • Real-life private investigation scenarios brought to life

Education Seminars	
e2e-assure **Elevating cybersecurity as a business enabler and source of competitive advantage** **Carl Urban,** Lead Cyber Consultant, e2e-assure	In this session, Carl will be discussing a paradigm shift in how organisations think of cybersecurity, to bring further business benefits above and beyond just being more secure. He'll be bringing together insights from recent conversations with customers, partners and industry experts as well as practical examples from industry on how to make this shift and give your organisation an additional element of competitive advantage over the competition. • Foundations for effective cybersecurity, including building the right culture • Effective communication with board members • Building trust through transparent communications • Benefits to organisations of viewing cybersecurity as more than just a cost centre • How organisations can make cybersecurity a new source of competitive advantage
GATEWATCHER **Understand the technologies required for the effective and efficient detection of cyber-threats to protect your organisation** **Ian Dutton,** Senior Sales Engineer, GATEWATCHER	• Providing a 360 degree view • What complementary detection technologies should you deploy? • Detecting low noise advanced attacks, including APTs and zero days
Hunters **Hunters: The SOC of the future** **Hanan Levin,** VP Sales EMEA, Hunters	Join Hunters to explore the key trends and paradigm shifts in data, detection and investigation, within the ever changing world of SOCs. • Find out how you can increase data retention whilst reducing your costs, through using built-in-detection and automation in your SOC platform
Imperva **Demystifying data protection: steps to find, monitor and control without chaos** **Adrian Clark,** Data Security Specialist, Imperva	Data security is one of the most complex security challenges to modern business. Leaders faced with structured, unstructured, and now, semistructured data have the herculean task of defending their data, while staying compliant with a litany of regional and global regulations. In this session, Adrian Clark will demystify some best practices in finding, monitoring, and controlling data regardless of where it lives. Walk away with steps you can take to secure your data without an army of people, a vault of cash, or a PhD. Attendees will: • Learn the difference between structured, unstructured and semistructured data • Understand why you should not simply monitor your most critical data when most breaches occur in areas where the stakes are much lower and the entry points are much easier to gain access to • Discover why real time security is too slow and why data classification should come second to monitoring when you begin a security overhaul
Intigriti **An Introduction to bug bounty programs for businesses** **Mark Wiley,** Senior Account Executive, Intigriti	Organisations without vulnerability disclosure policies are failing to address researchers' security warnings. The need for modern, proactive security has never been more important. A simple yet proven method to protect against cyber-threats is to invite ethical hackers in. Ethical hacker communities help to keep companies' data safe from cybercrime. But starting a collaboration with ethical hackers often begins with questions. Join our talk for insights to help your company get started with bug bounty programs. You'll learn: • What bug bounty programs are • How companies can work with ethical hackers • The difference between bug bounty programs and penetration tests

Education Seminars	
Malwarebytes **Threat disruption: Securing 2022 from 2021** **Kenny Williams,** Solution Engineer, Malwarebytes	In this presentation dive into the latest threat intelligence to: • Understand how COVID-19 caused a disruption of cybercrime that not only changed the trajectory of the landscape well into 2022 but shifted how we fight attacks today • Find out how global law enforcement has shifted the players in ransomware • Learn the most effective defence strategies to beef up your network security against emerging threats.
Netwrix **Streamlining compliance with zero standing privilege** **Anthony Moillic,** EMEA Field CISO, Netwrix	Many compliance standards require organisations to maintain control over privileged access, and this is a top area of focus by auditors and cybersecurity insurers. Although privileged accounts are a crucial part of day-to-day work for admins, most of them are only used for a short amount of time. The rest of the time they present risk in the face of your next compliance audit or cybersecurity insurance assessment. Join this session to learn: • How contemporary solutions reduce this risk only to some extent, while being costly and time-consuming to deploy • How simply managing accounts is risk-prone and does not address the problem completely • How to implement the zero standing privilege approach to simplify compliance and get cybersecurity insurance coverage
Obsidian Security **Cookies and Spam: Exploring MFA bypass techniques used by attackers to breach SaaS applications** **Chris Fuller,** Principal Product and Solutions Architect, Obsidian Security	Lapsus$ gained notoriety by breaking into some of the world's largest enterprises like EA, Microsoft and Okta. More recently, Uber and Rockstar Games suffered similar breaches. These are organisations with highly sophisticated security teams and widespread adoption of security best practices such as MFA, so how are attackers gaining access? In the wild, crude techniques such as 'MFA prompt spamming' and more advanced methods such as reverse phishing proxies can help motivated attack groups access sensitive data. This session will explore some of those techniques and discuss mitigation strategies in the context of SaaS applications. • Explore how session hijacking helps attackers bypass MFA and see how this data is sold in underground forums • See how attackers use session hijacking to intercept tokens and bypass MFA in a live demo • Learn how to identify and mitigate token compromise in SaaS applications
One Identity **A unified defence against identity sprawl threats** **Stuart Sharp,** Vice President of Solution Engineering, One Identity	• The role of AI in dynamic threat response • The value of consolidating identity management and security functions to one integrated platform • Closing security gaps via integrated risk flows
Red Sift **Email security & brand protection: Two sides of the same coin?** **Joshua Harris,** Senior Customer Success Engineer, Red Sift	• 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 behaviours

Education Seminars	
SentinelOne **Debunking common myths about XDR** **PJ Norris,** Senior Security Engineer, SentinelOne	There has been a tremendous buzz across the cybersecurity community about the emerging technology known as XDR (Extended Detection and Response). Unfortunately for the practitioner, there has yet to be a single definition widely accepted by both analysts and vendors purporting to be knowledgeable on the subject. Join this session to find out: • What is XDR and why should I consider the technology in my enterprise security stack? • What should I expect from vendors who claim to have built the perfect mousetrap? What is reality, and what is just hype? • What are some generally accepted value statements associated with XDR? • Allow us to debunk a few common myths that continue to muddy the water for security teams
SOCRadar **How to track your data on the dark web** **Samet Sazak,** Technical Account Manager, SOCRadar	As the most extensive worldwide system that stores information on everything (and almost everyone), the Internet comprises three distinct layers: the visible, the deep, and the dark web. Some layers contain significantly more information than others. The Internet is becoming more complicated, but it is also daunting. Given how little we know and how little control we have, it is fair to feel apprehensive, particularly when we encounter news and stories concerning the dark web. We automatically identify this menacing term with anything dangerous. In this seminar, you'll learn: • How to find out if your important data has been breached • The risks associated with that data falling into the wrong hands • Which markets, forums, and other corners of the dark web are most relevant right now • How to use intelligence to protect against credential leakage, data breaches, and ransomware attacks
Virtru **Embrace a new kind of security: Zero Trust Data Control** **Llewellyn Wells,** Solutions Consultant, Virtru	The digital world is now perimeter-less and the practice of cybersecurity is rapidly shifting from centralised, to decentralised policy controls. Up until now, Zero Trust security initiatives have focused primarily on identities, devices, networks, and apps. But what about data? Data is everyone's most valuable resource and what every attacker is after. It's constantly on the move – being downloaded, shared, copied, and modified. You can't afford to lock it down, and you can't afford to lose control of it Join Virtru as we discuss: • The importance of Zero Trust Data Control (ZTDC) • The benefits of adding policy controls that are capable of following data regardless of where it goes or how it is used • How you can rethink your cybersecurity stack with data at the core to protect your organisation's most important asset and prepare yourself to manage future cyber-threats