Post event report

e-crime & cybersecurity CONGRESS

The 18th e-Crime & Cybersecurity Congress

3rd & 4th March 2020 | London, UK

Strategic Sponsors

Attivo Networks
CrowdStrike
Darktrace
ExtraHop
Flashpoint
illumio
Intsights Defend Forward™
Menlo Security
netwrix
OneTrust Privacy – Privacy Management Software
Orange Cyberdefense
Telesoft
TrapX Security
zscaler™

Education Seminar Sponsors

Accellion
activereach
Check Point Software Technologies Ltd.
cybereason
Digital Guardian
digital shadows_
Forescout
Guardicore
Intel471
kaspersky
Kenna Security
Netacea
OneTrust Vendorpedia™ – Third-Party Risk Software
proofpoint
Rangeforce
Red Sift
RiskIQ
Swimlane
Synack
tripwire
wandera

Networking Sponsors

Agari
Reversing Labs
ThreatConnect

Branding Sponsors

cortida
Pulse Secure

“It was a well organised event and I very much enjoyed the presentations and educative sessions. Well done. I'd like to highlight the well balanced schedule with a good mix of themes and topics presented by a well selected group of specialists in their respective field. I am looking forward to attending future events.”

Director, Governance & Risk, Commerzbank

“Great presenters, great topics, well picked vendors, great venue = great event.”

Head of IT, The Ratcliffe Groves Partnership

“In spite of the media coverage on the Covid-19 outbreak both globally and locally, the e-Crime & Cybersecurity Congress was very well-attended. This is a testament of AKJ organising a high-quality event that is both topical and relevant to risk and cybersecurity professionals. The event provides ample opportunity to network with peers and vendors and the educational sessions provide more detailed information to the attendees on the specific topic of interest. As always this is one event that I make every effort to attend.”

IT Security & Risk Officer, UBS

“This was my third Congress. I enjoyed this well organised event, which always gives me fresh insights and ideas. I will definitely be back next year.”

UK Data Protection Officer and Deputy Group DPO, Stonehage Fleming

“For me the event was extremely useful in understanding where the vendor industry is going and to get insights into fellow professionals' thinking on areas close to the Information Security Professional's heart. Some really innovative approaches and the case-studies really worthy of a seat!”

Regional Information Security Officer EMEA, APAC and Japan, ION Group

“Excellent speakers and presentations with a very wide supplier participation, and opportunity to make and develop cross sector contacts.”

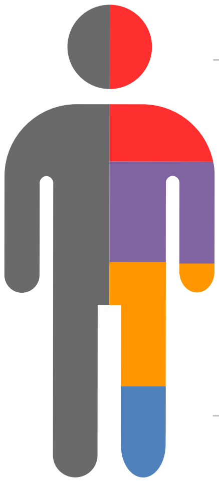
Director of Performance and Portfolio, Metropolitan Police Service

Inside this report:

Key themes

- Adapting to the changing threatscape
- Defining data, dealing with data
- Solving the problem of privileged access
- Next-generation threat and vulnerability management
- Connecting security, fraud and data management silos
- Securing digital transformation

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

Jose Alemán, Global Pre-sales Expert, Kaspersky; Michael Aydeniz, Head of Fraud and Credit Risk, Planet; Zsuzsanna Berenyi, Cyber Security Culture and Engagement Specialist, Refinitiv; Nathan Beresforde, Account Director, Darktrace; Stewart K. Bertram, Director of Intelligence, Digital Shadows; Terry Bishop, VP, Technical Services, RiskIQ; Simon Black, Pre-Sales Systems Engineer, Kenna Security; Adam Boynton, Sales Manager, Wandera; Adam Brady, Director Systems Engineering EMEA, Illumio; Robert Brooker, Co-Head of Fraud and Forensics, PKF Littlejohn; Dan Burns, Information Security Manager, NEXT; Joseph Byrne, Privacy Solutions Engineer – CIPP/E, CIPM, OneTrust; Simon Cross, Security Architect, Lloyds; Avishag Daniely, Director of Product Management, Guardicore; Trevor Dearing, Technical Director, EMEA, Illumio; Maxim Denizhenko, Lead Business Development, Enterprise Blockchain Security, Kaspersky; Jules Pagna Disso, Group Head of Cyber Risk Intelligence, BNP Paribas; Dean Ferrando, Lead Systems Engineer, Tripwire; Kevin Fielder, CISO, Just Eat; Lotem Finkelsteen, Head of Threat Intelligence, Check Point; Terje Aleksander Fjeldvaer, Head of Financial Cyber Crime Center, DNB; Nathan Gilks, Regional Solutions Architect, TrapX Security; Debbie Grant, Senior Policy Lead, Fraud Strategy & Criminal Disruption, Visa; Mark Greenwood, Chief Technical Architect, Netacea; Adam Gwinnett, Head of Strategy, Enterprise Architecture & Cyber Security, Metropolitan Police; Deborah Haworth, CISO, Penguin Random House; Alphus Hinds, CISO, Standard Bank; Detective Sergeant Ben Hobbs – DCPCU, Dedicated Card & Payment Crime Unit, Metropolitan Police; Mike Hulett, Head of Operations, National Cyber Crime Unit (NCCU); Federico Iaschi, Head of Information Security, Seqirus; Akhil Lalwani, Head of Digital Platforms, Prudential; Gordon Lawson, CRO, President, RangeForce; Jonathan Lee, Sr. Product Manager, Menlo Security; Matt Logan, Vice President of Field Engineering – EMEA, Digital Guardian; Maurits Lucas, Director of Intelligence Solutions, Intel 471; Alan MacGillivray, Account Executive, OneTrust; Max Mansson, Director, UK & Europe, Silobreaker; Etay Maor, Chief Security Officer, IntSights; Dave Matthews, Systems Engineer, Netwrix; Goher Mohammad, Head of Information Security, L&Q Group; Jamie Moles, Senior Security Engineer, ExtraHop; Roy Murdoch, SE Manager UKISA, Proofpoint; Richard Orange, Regional Director UKI, Forescout Technologies; Michael Owen, Head of Systems Engineering UK&I, IntSights; Nick Palmer, Technical Director, Attivo Networks; Mariana Pereira, Director of Email Security Products, Darktrace; Danny Phillips, Senior Manager of Systems Engineering, Zscaler; Becky Pinkard, CISO, Aldermore Bank; Tom Platt, Senior Account Manager, Netacea; Vijay Punja, Technical Account Manager, RiskIQ; Brett Raybould, EMEA Solutions Architect, Menlo Security; Stephen Roostan, VP EMEA, Kenna Security; Martin Rudd, Chief Technology Officer, Telesoft Technologies; Garry Scobie, Deputy CISO, The University of Edinburgh; Justin Shaw-Gray, Account Director, Synack Inc.; Mark Smith, Pre-Sales Manager, Orange Cyberdefense; Rois Ni Thuama, Head of Cybersecurity Governance & Legal Partnerships, Red Sift; Kevin Tongs, Director Customer Success (EMEA), Flashpoint Intel; Toby Van de Grift, UK Regional Director, Swimlane; Anthony Wainman, Senior Sales Engineer, Cybereason; Mark Ward, Senior Solutions Architect, CrowdStrike; Sam Watling, Information Security Governance and Compliance Lead, TUI; Harry Zorn, Vice President Sales, EMEA, Accellion

Agenda | Day 1 | 3rd March 2020

08:00 Registration and breakfast networking

08:50 Chairman's welcome

09:00 **The innovation juggernaut: making security leaders partners in success**

Akhil Lalwani, Head of Digital Platforms, Prudential

- Being a part of the innovation journey: How can today's CISO ensure they are active partners in the journey?
- Innovation and customer needs are constantly changing – can our approach to security remain static?
- Takeaways: the actionable five step framework

09:20 **Defence in diversification: improving cybersecurity through smart consolidation**

Jamie Moles, Senior Security Engineer, ExtraHop

- How a data-first approach to security architectures can illuminate natural consolidation points
- How collaboration with other parts of the IT organisation can improve security posture and reduce tool sprawl
- How this collaborative approach also creates an opportunity to leverage other parts of the organisation to improve security posture through smarter processes and practices

09:40 **Preparing for the next cyber-attack – from the attacker's perspective**

Etay Maor, Chief Security Officer, IntSights

- Cybersecurity solutions often utilise the latest 'AI, machine learning driven, blockchain based, next gen, highly granular, zero trust, future proof technology... as a service'. However, looking at the common themes in the major breaches it looks like cyber-adversaries have a different approach to their attacks
- How our adversaries conduct threat intel gathering and attack preparation, explored through case studies detailing how security breaches are (easily) performed
- How current attack mapping frameworks can be used to prepare for the next attack

10:00 **Collaborative criminal combat. How collaboration between law enforcement and industry is critical to protect us from evolving cyber-threats**

Debbie Grant, Senior Policy Lead, Fraud Strategy & Criminal Disruption, Visa, and
Detective Sergeant **Ben Hobbs** – DCPCU, Dedicated Card & Payment Crime Unit, Metropolitan Police

- Fraud as a catalyst for other forms of high-level crime. The relationship between fraud, AML and cybersecurity, and how the digitalisation of business is making the challenges and risks experienced by all three increasingly interlinked
- Public and private collaboration and how working together can have an impact on disrupting criminal activities
- Real-life case studies and insights into the evolution of social engineering

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

Accellion	**Third-party communication for confidentiality, compliance and control** **Harry Zorn,** Vice President Sales, EMEA, Accellion
CrowdStrike	**e-Crime and the frontline: lessons learnt in responding to the most advanced cyber-attacks** **Mark Ward,** Senior Solutions Architect, CrowdStrike
Kenna Security	**Risk-based, time-critical vulnerability management: four steps for success** **Stephen Roostan,** VP EMEA, Kenna Security, and **Simon Black,** Pre-Sales Systems Engineer, Kenna Security
Netacea	**Bad Bots 101: how to carry out an ATO attack** **Mark Greenwood,** Chief Technical Architect, Netacea, and **Tom Platt,** Senior Account Manager, Netacea
RiskIQ	**Using internet reconnaissance data to defend against targeted attacks** **Vijay Punja,** Technical Account Manager, RiskIQ
TrapX Security	**Building an effective deception strategy** **Nathan Gilks,** Regional Solutions Architect, TrapX Security
Tripwire	**The future is hybrid: key considerations for cloud and DevOps** **Dean Ferrando,** Lead Systems Engineer, Tripwire
Wandera	**Redefining the edge: making the most of your security investments in a zero-trust world** **Adam Boynton,** Sales Manager, Wandera

11:00 Networking and refreshments

11:30 **The hyper-connected CISO: inconvenient truths and lessons on staying afloat**

Becky Pinkard, CISO, Aldermore Bank

- How digitalisation, of both the financial services and also of the general business landscape, has impacted the information security remit, and how you can secure a hyper-connected world
- The CISO's role in this ever-evolving landscape
- The mandatory changes and evolution required around security awareness across the workforce

11:50 **The hidden adversary. Advanced detection of attackers on the network using deception**

Nick Palmer, Technical Director, Attivo Networks

- Understand how attackers can breach even the most well fortified networks
- Discover how quickly attackers can move towards monetisable targets in an organisation
- Learn how deployment of advanced detection techniques can uncover hidden attackers
- See how integration with existing tooling and SOC workflows can contain threats and minimise risk

12:10 **ISO27001 & the GDPR: identifying overlap and streamlining efforts**

Joseph Byrne, Privacy Solutions Engineer – CIPP/E, CIPM, OneTrust

- Map the most common security operations standard, ISO 27001 to the world's most influential piece of privacy legislation, the GDPR
- Identify how much work toward GDPR compliance that security teams have likely already done
- Outline six main areas of common ground that should help every organisation align their security and privacy operations
- Develop a framework to reduce the risk of a damaging incident while increasing productivity and customer trust
- Understand the importance of building a cohesive compliance strategy across privacy and security teams
- Learn about the stakeholders, teams, tools and processes that should come together for a comprehensive privacy and security strategy
- Take away a roadmap and action plan for bridging privacy and security in your organisation

12:30 **Faking it: combatting email impersonation with AI**

Mariana Pereira, Director of Email Security Products, Darktrace

- 'Impersonation attacks' are on the rise, as AI is increasingly being used to automatically generate spear-phishing emails, or 'digital fakes'
- Humans can no longer distinguish real from fake on their own, so businesses are increasingly turning to AI to distinguish friend from foe and fight back
- Learn how 'immune system' technology can stop cyber-threats before any damage is done

Agenda | Day 1 | 3rd March 2020

12:50	**Education Seminars | Session 2**	
	Attivo Networks	**Operationalising deception. How to conceive, execute and integrate advanced threat detection into your organisation** **Nick Palmer,** Technical Director, Attivo Networks
	Digital Guardian	**Visibility is key to a successful data protection programme** **Matt Logan,** Vice President of Field Engineering – EMEA, Digital Guardian
	Guardicore	**Beyond the (fire)wall** **Avishag Daniely,** Director of Product Management, Guardicore
	Kaspersky	**To blockchain or not to blockchain** **Maxim Denizhenko,** Lead Business Development, Enterprise Blockchain Security, Kaspersky
	Menlo Security	**Internet isolation: a key requirement for the modern security architecture** **Brett Raybould,** EMEA Solutions Architect, Menlo Security
	Proofpoint	**Building a people-centric security strategy** **Roy Murdoch,** SE Manager UKISA, Proofpoint
	Red Sift	**Lessons from the dark side?** **Rois Ni Thuama,** Head of Cybersecurity Governance & Legal Partnerships, Red Sift
	Zscaler	**How you can achieve a zero trust network access** **Danny Phillips,** Senior Manager of Systems Engineering, Zscaler
13:30	Lunch and networking	
14:30	**Critical intel on threat intel. Fraud threat intelligence and the business benefits and ROI**	
	Terje Aleksander Fjeldvaer, Head of Financial Cyber Crime Center, DNB • Insight into how criminals use technology and the increased complexity of cases • How organised criminal groups cynically defraud and exploit peoples weaknesses for financial gain • The connection between fraud and terrorism • How we work on fraud threat intel and the business benefits and ROI	
14:50	**The latest state of the threat: attack is inevitable, compromise is probable, engagement is essential**	
	Mark Smith, Pre-Sales Manager, Orange Cyberdefense • Security strategies are many times driven on fear and compliance issues, with spending on perceived rather than genuine threats • Understanding the real threat in a world that is highly complex and changing all the time is not a simple task • In this session, discover Orange Cyberdefense's research on how threat is evolving and where you should be spending energy and focusing on	
15:10	**A first, practical step to a zero trust strategy**	
	Trevor Dearing, Technical Director, EMEA, Illumio • Computing environments are becoming so diverse and security so sophisticated that trying to keep them synchronised is now a huge issue • Many agencies and governments have adopted zero trust as the easiest way for organisations to adopt a culture of safe and secure operation • There is a perception that zero trust can be complex and expensive. In this session, we will look at how the basics can be achieved, with very little impact on existing infrastructure, to take the first steps toward a zero trust environment.	
15:30	**Education Seminars | Session 3**	
	Digital Shadows	**Information warfare – what is it and how does it affect me?** **Stewart K. Bertram,** Director of Intelligence, Digital Shadows
	Intel 471	**Extra! Extra! Read all about it! The evolving sophistication of how threat actors are using current news events to spread malware** **Maurits Lucas,** Director of Intelligence Solutions, Intel 471, and **Max Mansson,** Director, UK & Europe, Silobreaker
	OneTrust	**Transitioning GDPR from a compliance checklist to 'business as usual'** **Joseph Byrne,** Privacy Solutions Engineer, CIPP/E, CIPM, OneTrust
	Swimlane	**SOAR in the age of DX** **Toby Van de Grift,** UK Regional Director, Swimlane
	Synack	**Using hackers to beat hackers: innovation at Just Eat** **Justin Shaw-Gray,** Account Director, Synack Inc., and **Kevin Fielder,** CISO, Just Eat
16:10	Networking and refreshments	
16:30	**EXECUTIVE PANEL DISCUSSION**	**Breaking down barriers, solving the cyber conundrum**
	Chaired by: Alphus Hinds, CISO, Standard Bank **Zsuzsanna Berenyi,** Cyber Security Culture and Engagement Specialist, Refinitiv **Deborah Haworth,** CISO, Penguin Random House **Adam Gwinnet,** Head of Enterprise Architecture & Cyber Security, Metropolitan Police Service **Nicola Lishak,** Head of Information Assurance, Royal Mail	
16:50	**Extending data security to the cloud**	
	Dave Matthews, Systems Engineer, Netwrix • What specific challenges are there for securing data in the cloud? • How can a single data security strategy be applied to the entire hybrid IT environment? • What steps can help you protect your data across your on-premises and cloud-based systems?	
17:10	**'Will' vs. 'Skill': are we using the wrong tactics to recruit for our information security team?**	
	Goher Mohammad, Head of Information Security, L&Q Group • There is a cybersecurity skills shortage that is still not shrinking, as hiring managers and leaders we need to tackle the gap between demand and supply of cybersecurity professionals • Traditional methods of hiring need challenging, how to adopt an agile and flexible approach • Get yourself noticed! What are cybersecurity hiring managers looking for in a new recruit? • Positive results: lessons learnt from L&Q Group on building and retaining talent within your security team	
17:30	Networking and drinks reception	
18:30	End of day one	

Agenda | Day 2 | 4th March 2020

08:00	Registration and breakfast networking	
08:50	Chairman's welcome	
09:00	**Ransomware: an evolving threat**	
	Mike Hulett, Head of Operations, National Cyber Crime Unit (NCCU) • What are the most prevalent forms of ransomware, and common attack methodologies • How has the threat and the market evolved over the last couple of years • A case study – what might happen to you, and how law enforcement may assist • How can you avoid this? Best practice for security & resilience	
09:20	**Untangling the spider's web: e-crime exposed**	
	Mark Ward, Senior Solutions Architect, CrowdStrike • Understanding the threat landscape, who the adversaries are and how we can spot them • Examining the latest attack techniques adopted and deployed by e-crime actors • How we use the intelligence we gather about the adversary to prevent, protect and respond against the cyber-threat of tomorrow	
09:40	**Deception in action: how deception helped one of the largest global brands transform its cyber-resilience programme**	
	Tony Kinkead, Regional Director – EMEA, TrapX Security • Why do defenders have to be right 100% of the time? How do you turn the odds in your favour? • Improving detection of the external intruder, zero-day malware and the insider threat • Reducing alert fatigue, false positives and dead ends for critical resources • Incorporating detection for IoT, OT and legacy systems across the enterprise	
10:00	**Managing fraud in an unregulated market**	
	Michael Aydeniz, Head of Fraud and Credit Risk, Planet • Navigating the myriad challenges faced by an organisation when they operate in a largely unregulated market • Managing cross-jurisdictional fraud issues • First-hand case study taken by Planet in devising a one-size-fits-all approach to fraud monitoring and mitigation	
10:20	**Education Seminars | Session 4**	
	Cybereason	**A live cyber-attack simulation** **Anthony Wainman,** Senior Sales Engineer, Cybereason
	Forescout Technologies	**Device visibility and control: transforming enterprise-wide network segmentation** **Richard Orange,** Regional Director UKI, Forescout Technologies
	Illumio	**Decoupling security segmentation from network infrastructure** **Trevor Dearing,** Technical Director, EMEA, Illumio, and **Adam Brady,** Director Systems Engineering EMEA, Illumio
	Netwrix	**Back to the future: a data breach prevention plan** **Dave Matthews,** Systems Engineer, Netwrix
	OneTrust	**Overcoming today's most common security & privacy challenges** **Alan MacGillivray,** Account Executive, OneTrust
	RangeForce	**The RangeForce 'Cyber Gym': building cybersecurity muscle memory through simulated training for enterprise tech teams** **Gordon Lawson,** CRO, President, RangeForce
11:00	Networking and refreshments	
11:30	**EXECUTIVE PANEL DISCUSSION**	**Threat intelligence in the real world**
	Jules Pagna Disso, Group Head of Cyber Risk Intelligence, BNP Paribas **Simon Cross,** Security Architect, Lloyds **Dan Burns,** Information Security Manager, NEXT **Martin Rudd,** Chief Technology Officer, Telesoft Technologies	
11:50	**Achieve security without compromise**	
	Jonathan Lee, Sr. Product Manager, Menlo Security • Why legacy appliance-based security is not going to cut it in the age of cloud • Why a detection based, 'almost safe' approach has its limitations • Why we should challenge Gartner's adaptive security architecture with a new technology • Learn how isolation makes it possible to approach security and networking in an entirely new way	
12:10	**The intelligence lifecycle, dissemination, and why compromised credentials are paramount**	
	Kevin Tongs, Director Customer Success (EMEA), Flashpoint Intel • A summary of the intelligence lifecycle • The rules of dissemination within the cycle • How these rules have influenced Flashpoint's product development • Why compromised credential monitoring is key to timely, actionable intelligence	
12:30	**Making a cloud-first strategy a reality**	
	Danny Phillips, Senior Manager of Systems Engineering, Zscaler • Legacy IT debt, unfinished upgrades and compliance are all quoted as reasons to delay cloud adoption • So if you were able to start your business again from scratch, and plan the next five-year IT strategy, what would it consist of? • With technology shifts such as the move to cloud, are current security policies still valid? • Join our session to discover how you can implement a cloud-first strategy amidst legacy architectures	
12:50	**Education Seminars | Session 5**	
	Check Point	**Cyber warfare 2019/2020** **Lotem Finkelsteen,** Head of Threat Intelligence, Check Point
	Darktrace	**Offensive AI vs. Defensive AI: battle of the algorithms** **Nathan Beresforde,** Account Director, Darktrace
	ExtraHop	**Winning strategies to scale and upskill your security team** **Jamie Moles,** Senior Security Engineer, ExtraHop
	IntSights	**Shutting down attacks with dark web intelligence** **Michael Owen,** Head of Systems Engineering UK&I, IntSights
	Kaspersky	**Hunting the hunters** **Jose Alemán,** Global Pre-sales Expert, Kaspersky
	RiskIQ	**Defending your organisation against JavaScript injection attacks** **Terry Bishop,** VP, Technical Services, RiskIQ

Agenda | Day 2 | 4th March 2020

13:30	Lunch and networking
14:30	**The big blue button – a law enforcement lens on cybercrime response**
	Adam Gwinnett, Head of Strategy, Enterprise Architecture & Cyber Security, Metropolitan Police • A call to arms: bringing cyber from passive FUD to active engagement • Reporting and greater disclosure from industry. Why have we got to the point where c. 99% of fraud cases across financial services go unreported? • Actionable lessons from law enforcement on ‘when to push the big blue button’
14:50	**How do you prioritise cybersecurity resources and budget? Metrics and ROI for a cyber-secure culture**
	Federico Iaschi, Head of Information Security, Seqirus • Training and awareness: how do you prove ROI, budget and metrics for a cyber-secure culture? • Key ‘action item’ breakouts to help an information security awareness programme mature and thrive • The particular risks and consequences of the bio-pharma industry. Supply chain risk, and the physical, ‘real world’ consequences of a breach
15:10	**The F word: making fraud and forensics a key business priority in the digital world**
	Robert Brooker, Co-Head of Fraud and Forensics, PKF Littlejohn • Actionable insights into current fraud, bribery and corruption risks and the impact of digitalisation • The relationship between corporate fraud, governance and cyber, and why collaboration between the three is vital for the business • How do you get buy in from the C-suite, and how can you implement change in the behaviours and culture of a business?
15:30	Networking and refreshments
15:50	**Cybercrime and the movies. Why cyber needs a makeover**
	Garry Scobie, Deputy CISO, The University of Edinburgh • Cybersecurity is viewed as a complex game of cat and mouse, played out against men in darkened rooms wearing sunglasses and hoods. The movies perpetuate this myth • Does this portrayal of cybercrime hinder the recruitment of diverse security minded individuals to tackle the problem? • Behind the scenes: how the movies compare with the reality of cybercrime. How can we use this disconnect to become security savvy in our on-line lives? • Cybersecurity needs a makeover so let’s walk-through some classic movies and see how they fare against the real threats we face today
16:10	**Actionable cyber-awareness. Time for real change**
	Sam Watling, Information Security Governance and Compliance Lead, TUI • How to inspire your colleagues to make real change in the way they secure themselves personally and therefore protect your business • Why TUI embarked on their award-winning colleague awareness and behavioural change programme across a multi-cultural, multi-language, geographically distributed workforce • How a common theme and purpose has driven tangible behavioural change across the business • How to adopt security best practice and behaviours at home and at work, protecting colleagues, families and reducing risk to the company as a whole
16:30	Congress close

Education Seminars

Accellion

Third-party communication for confidentiality, compliance and control

Harry Zorn, Vice President Sales, EMEA, Accellion

In this presentation delegates will learn different techniques and ideas how to reduce third-party risk.

What delegates will learn:

- The evolution from network to application to content firewall
- How to increase the level of security by making life easier
- Whether or not a newspaper is a good weapon of choice in a knife-fight
- How to decrease third-party risk
- How to consolidate security technologies, reduce risk and save money

Attivo Networks

Operationalising deception. How to conceive, execute and integrate advanced threat detection into your organisation

Nick Palmer, Technical Director, Attivo Networks

When the decision has been taken to deploy deception to augment the organisation's security posture, several key questions are raised, which must be addressed to properly leverage value from this critical detection capability. By planning how to deploy deception, matched to organisational risk appetite, integrated into pre-existing SOC workflows and designed to support incident response, security teams can make extremely effective use of deception to understand how and where attackers have managed to breach the network. Additionally, their motives and methods can be more effectively understood to properly plan for future events and take the power from the attackers and place it in the hands of the SOC teams.

- Understand deception maturity – crawl, walk run
- Understand how to deploy deceptive assets and fake data
- Understand the critical integrations and how to gain 360 degree visibility of attackers on the network
- Engage the business in building effective deception campaigns and gain stakeholder commitment to deception

Check Point

Cyber warfare 2019/2020

Lotem Finkelsteen, Head of Threat Intelligence, Check Point

2019 presented a complex threat landscape where nation states, cybercrime organisations, and private contractors accelerated the cyber-arms race, elevating each other's capabilities at an alarming pace.

In our session, we will try to cover the trends that characterised 2019 and may design the threat landscape of 2020, supported with real-world cases and data.

- See how the threat intelligence team unravels cybercrimes
- Real cases step by step footage – from the first hunch to the hacker identity
- Learn how you can identify the first signs of a breach

CrowdStrike

e-Crime and the frontline: lessons learnt in responding to the most advanced cyber-attacks

Mark Ward, Senior Solutions Architect, CrowdStrike

Defending against modern adversaries requires the ability to detect and understand threats quickly and to respond decisively. CrowdStrike's experts fight and win these battles every day, and have one of the industry's most comprehensive pictures of today's top cyber-threats. Allow us to lead you through a deep dive into global observations and trends, and real-world intrusion case studies, delivering deep insights on modern adversaries, and their tactics, techniques, and procedures (TTPs).

- Lessons learnt in the course of conducting in-depth digital forensics, IR and remediation with real-world strategic insight into the current threat landscape
- How advanced attacks succeed in evading modern defences
- How applied threat intel can deliver advantage in protecting your enterprise

Cybereason

A live cyber-attack simulation

Anthony Wainman, Senior Sales Engineer, Cybereason

In today's world, preventing a cyber-attack is difficult and penetration is inevitable. We – the defenders need to find other ways of protecting our organisations. In this session, you will gain insight in the motivations of attackers and see how world class defenders are using their skills and tools in the most efficient and smartest way.

In this session, you will:

- Witness the attacker's infiltration
- See the malicious operation as it moves across the entire environment
- Understand how you can gain the upper hand and learn why current security trends are failing

Education Seminars

Darktrace

Offensive AI vs. Defensive AI: battle of the algorithms

Nathan Beresforde, Account Director, Darktrace

Among rapidly evolving technological advancements, the emergence of AI-enhanced malware is making cyber-attacks exponentially more dangerous and harder to identify. In the near future, we will begin to see supercharged, AI-powered cyber-attacks leveraged at scale. To protect against offensive AI attacks, organisations are turning to defensive cyber AI, which can identify and neutralise emerging malicious activity, no matter when, or where, it strikes.

In this session, learn about:

- Paradigm shifts in the cyber-landscape
- Advancements in offensive AI attack techniques
- The Immune System Approach to cybersecurity and defensive, autonomous response capabilities
- Real-world examples of emerging threats that were stopped with Cyber AI

Digital Guardian

Visibility is key to a successful data protection programme

Matt Logan, Vice President of Field Engineering – EMEA, Digital Guardian

Data protection programmes should never fail if you use the right tools! Gone are the days of guessing what you need to protect, deploying policies in an hope and pray fashion.

Digital Guardian uses advanced visibility to provide you with a detailed view of exactly how data flows and is being used in your organisation.

Additionally, why combining data protection and endpoint detection and response combined is the future of data protection.

In this session you will learn:

- How to start a successful data protection programme
- Avoiding the pit falls
- Using advanced data protection technologies to show you how data is being used
- DLP and EDR, why combine

Digital Shadows

Information warfare – what is it and how does it affect me?

Stewart K. Bertram, Director of Intelligence, Digital Shadows

Information warfare is an umbrella term for an amorphous collection of activities that fall under the banner of terminology such as 'phycological warfare', 'fake news', 'disinformation', 'misinformation', and any number of other increasingly complex terms. With recent events such as the United States election in 2016 and the recent developments around Brexit, information warfare is undoubtably an important issue. But where to start with this subject, and is it even a cybersecurity issue?

This talk seeks to address this issue and dissect information warfare as a concept by offering a range of taxonomies to analyse the subject, backed up by several real-world cyberspace case studies.

Topics examined include how threat actors realise information warfare campaigns both at a conceptual level and a practical level, making use of tactics such as data theft and mobilisation via social media platforms.

The paper is both an introduction to the subject as well as a detailed primer for further work within research into the subject.

Key takeaways:

- What information warfare is and how it differs from propaganda and other forms of influence operations
- How cyberspace effects the practise of information warfare on a macro level
- How this abstract concept has the potential to develop into a genuine threat in the future
- The positive and negative aspects of information warfare from the adversary perspective

Education Seminars

ExtraHop

Winning strategies to scale and upskill your security team

Jamie Moles, Senior Security Engineer, ExtraHop

Businesses these days often face two main challenges: they have too much technology and they don't have the people to manage it. This requires new ways to make their security layers more effective and to scale their human and technology resources in the face of a growing threat landscape. In this session, we will discuss the challenges and opportunities facing security and IT teams when it comes to scaling their cybersecurity talent, and how they can train and 'upskill' staff members to address the problems of the enterprise.

Key discussion points will include:

- How to efficiently train and retain high-calibre cybersecurity professionals
- The part machine learning can play to alleviate alert fatigue and focus on what really matters
- Strategies for increasing collaboration between Security and Network Operations teams.

Forescout Technologies

Device visibility and control: transforming enterprise-wide network segmentation

Richard Orange, Regional Director UKI, Forescout Technologies

While network segmentation is not new, it is probably the best defence against the growing number of security threats and the best way to enable zero-trust policies. The real question is why are organisations so slow in adopting it?

In this session we will address the need to:

- Have full context of all connected devices and applications across the entire enterprise from campus to datacentre to cloud and OT environments
- Know and visualise traffic flows: map traffic flows to logical taxonomy of users, applications, services and devices
- Design and simulate segmentation policies to learn impact before enforcement
- Monitor segmentation hygiene real time and be able to respond to policy violations

Guardicore

Beyond the (fire)wall

Avishag Danielу, Director of Product Management, Guardicore

The age of the hybrid cloud has created a need for a different approach when it comes to firewalls. For some, virtual cloud firewalls seemed like they might be the answer to protecting the modern hybrid data centre, but the truth is, these are also insufficient for today's e-crime landscape.

This presentation will cover the main points firms need to take into consideration when choosing the right solution when securing its data centres, including:

- Latency
- Ease of deployment
- Maintenance and more

Illumio

Decoupling security segmentation from network infrastructure

Trevor Dearing, Technical Director, EMEA, Illumio, and **Adam Brady,** Director Systems Engineering EMEA, Illumio

Segmentation is the cornerstone of security and with many technologies it is hard to achieve. If you are trying to achieve this by handcrafting VLANs or using SDN you will already know how hard it can be. If segmentation is shackled to your physical or virtual network then you lose the ability to segment by role, application, environment or location which makes expanding to the cloud or containers very hard. If you can decouple segmentation from the network then things become not hard. You will have the capability to provide strong security independent of platform or network. In this session learn more about simple segmentation.

Bullet points:

- Network segmentation was designed to allow data traffic to move fast, not secure your servers and applications
- Security segmentation prevents lateral network traffic and protects your applications
- Application architects do not know how their systems are deployed in the network, and so cannot implement countermeasures against cybercriminals.
- Data centres often lack the necessary security mitigation systems, putting your high-value applications at great risk

Education Seminars

Intel 471

Extra! Extra! Read all about it! The evolving sophistication of how threat actors are using current news events to spread malware

Maurits Lucas, Director of Intelligence Solutions, Intel 471, and **Max Masson,** Director, UK & Europe, Silobreaker

Increasingly, threat actors are aligning their activities to high-profile global events, such as CoronaVirus, natural disasters, etc, to prey upon the fear and uncertainty stemming from mass media coverage of these events. This leads people to lower their state of alertness and do things that they wouldn't typically do, such as clicking links or attachments in emails they don't recognise. Though phishing is nothing new, the level of sophistication in threat actors' methods continually adapts and advances.

In this presentation, we will discuss:

- Insight into campaigns targeting the public's fear and uncertainty regarding CoronaVirus
- The methods threat actors are using to mask their activities and bypass individuals' own security awareness
- The recent evolving state changes of prolific malware families that provide insight into how actors are changing their targeting and delivery
- The identification of new connections among various actors and malware families that have not been seen before, which can help indicate new methods and campaigns that may soon emerge

IntSights

Shutting down attacks with dark web intelligence

Michael Owen, Head of Systems Engineering UK&I, IntSights

Threats originate from many different sources, some more obfuscated than others. In today's connected world, protecting your business is a full-time job and time is your most valuable asset. The dark web is one area from which many threats can originate, and monitoring these sources for intelligence related to your business can give you a vital heads-up on potential threats.

In this education session, we will explore some of those dark web sites and see where those threats could originate from and how you can use that intelligence to better protect yourself and your business.

Learning points:

- Expand your awareness of some of the dark web sites
- Understand how data is bought and sold
- Identify how this data can be used to decrease your risk threshold and increase your security

Kaspersky

To blockchain or not to blockchain

Maxim Denizhenko, Lead Business Development, Enterprise Blockchain Security, Kaspersky

Practical cybersecurity reasonings of blockchain-based solutions.

- Key features of blockchain technology
- Cybersecurity threats in blockchain solutions and how to mitigate them
- Does DLT always mean trust?
- Case studies

Kaspersky

Hunting the hunters

Jose Alemán, Global Pre-sales Expert, Kaspersky

Learn how leading global experts go from threat identification to actor attribution with the newest and most sophisticated tools.

In this session, we will provide real-life examples on how to track and identify attacks, providing insights about who is the actor behind the threat, adding threat attribution to threat intelligence as the last link in the chain.

- How to use threat intelligence to identify the most advanced threats in the world
- Step by step guide on how to perform an investigation based on real malware samples of very well-known attacks
- Exclusive premier of how our experts identify the actors behind the threats

Education Seminars

Kenna Security

Risk-based, time-critical vulnerability management: four steps for success

Stephen Roostan, VP EMEA, Kenna Security, and **Simon Black,** Pre-Sales Systems Engineer, Kenna Security

Join Steve and Simon to find out how leveraging data science through the lens of cyber-risk can quickly deliver multiple value streams across an organisation. This session will show how to empower security, DevOps, and management with a self-service portal that both improves cybersecurity, and delivers measurable efficiency gains to both IT security and development teams.

- Assessing the scale of the problem
- Benchmarking against industry metrics
- Establishing how success should be measured
- Deploying a self-service portal to enable ITOps/DevOps to be part of the remediation task force

Menlo Security

Internet isolation: a key requirement for the modern security architecture

Brett Raybould, EMEA Solutions Architect, Menlo Security

Organisations should not need to accept the short comings of solutions that cannot solve the problems of inbound threats via web and email. Isolation provides a secure execution environment where content can be executed away from the user and in a way that makes it impossible for the attacker to reach their target, thereby mitigating all risk from infection. Isolation also does not suffer from false positive or negatives. In the session, participants will learn how this is possible and how it solves many specific use cases. There will also be a live demo of Menlo Security's Cloud Proxy Platform, the first of its kind with an Isolation Core™.

What will attendees learn:

- Why isolation can achieve secure cloud transformation
- How to eliminate all risk of infection from browser based threats
- How to protect the user from credential theft via phishing attacks

Netacea

Bad Bots 101: how to carry out an ATO attack

Mark Greenwood, Chief Technical Architect, Netacea, and **Tom Platt,** Senior Account Manager, Netacea

Bots account for more than 50% of all online traffic and are responsible for a range of good, bad and nuisance activity. Consumers and businesses alike are exposed to bot risks, with the attackers able to carry out a range of illicit and often fraudulent activity.

- To highlight the significant, detrimental impact of bots targeting global enterprises, Netacea will simulate a real-time account takeover attack. The attack will demonstrate the ease with which a threat actor can orchestrate an account takeover that bypasses traditional security measures
- Throughout the attack, we will discuss the impact on various departments throughout an organisation – from security and operations to marketing managers – with reference to bot management best practices

Netwrix

Back to the future: a data breach prevention plan

Dave Matthews, Systems Engineer, Netwrix

When was the last time you saw a headline about an organisation falling victim to a costly cyber-attack? Yesterday? The day before? Have no doubt – your company is also a target.

In this session, you'll learn how to minimise the risk of a data breach, and how to survive your day if the worst does come to pass. Don't simply dream for a time machine when it's too late; come find out the secret to preventing breaches. If our calculations are correct, we should meet you at this educational seminar!

This session will outline the following:

- Your worst day: How to deal with a breach
- Your best defence: How to minimise the risk of a breach
- The secret to preventing breaches

Education Seminars

OneTrust

Transitioning GDPR from a compliance checklist to 'business as usual'

Joseph Byrne, Privacy Solutions Engineer, CIPP/E, CIPM, OneTrust

While privacy pros across the globe overhauled business processes leading up to the GDPR's effective date, 25th May 2018 was just the beginning. Compliance is an ongoing exercise and privacy must be integrated into every aspect of the business. In this session, we'll share strategies for shifting your GDPR programme from a compliance checklist item into 'business as usual' within your company. From privacy champions across the business to privacy by design, we'll outline a step-by-step approach to making privacy a reflex (and not a nuisance) to business operations and build privacy as a culture within your company.

- Understand how to shift GDPR compliance efforts from a one-off activity into business as usual
- Take home a step-by-step approach to ongoing GDPR compliance within your company
- Realise how ongoing GDPR efforts can set your company up for success with other global privacy laws

OneTrust

Overcoming today's most common security & privacy challenges

Alan MacGillivray, Account Executive, OneTrust

Managing third-party vendor risk before, during and after onboarding is a continuous effort under global privacy laws and security regulations. While outsourcing operations to vendors can alleviate business challenges, managing the associated risk with manual tools like spreadsheets is complex and time consuming. To streamline this process, organisations must put procedures in place to secure sufficient vendor guarantees and effectively work together during an audit, incident – or much more.

In this session, we'll breakdown a practical approach for automating third-party vendor risk management and explore helpful tips and real-world practical advice to automate third-party privacy and security risk programmes.

- Review the drivers and challenges organisations face when managing third-party vendor risk
- Identify priorities before, during and after vendor procurement
- Takeaway a six-step approach for automating the third-party vendor risk lifecycle
- Hear real case studies from privacy experts on how to practically tackle the third-party vendor risk

Proofpoint

Building a people-centric security strategy

Roy Murdoch, SE Manager UKISA, Proofpoint

Cybercriminals target employees with access to the information they need through highly sophisticated and personalised attacks. We will explore how cybercriminals use two of the most powerful information tools – LinkedIn and Google – to perform reconnaissance on potential targets. These social engineering techniques mean that attackers often know more about your employees than you do.

The only security strategy that will successfully combat today's advanced attacks is one that focuses on protecting your people.

This session explores how to build a strategy that:

- Reveals who is targeted and how
- Combats attacks before they reach your users
- Mitigates damage from the attacks that inevitably will reach your people
- Protects the data they create

RangeForce

The RangeForce 'Cyber Gym': building cybersecurity muscle memory through simulated training for enterprise tech teams

Gordon Lawson, CRO, President, RangeForce

Continuous professional development is crucial to keeping technically focussed teams ahead of the game. CISOs, VPs and Team Leads must also be able to establish baselines of skill levels within those teams, in order to identify any possible coverage gaps that could represent a threat to the organisation.

With the RangeForce on-demand, 100% cloud-hosted cybersecurity skills training platform, customers can:

- Acquire technical security skills online. Affordable and always accessible from any browser
- Learn essential real-world skills. From security operations to forensics to secure DevOps, training modules cover a breadth of mission-critical topics
- Learn how to defend against advanced attacks, quickly recognise and fix vulnerabilities
- Get actionable insights about performance and skill levels of team members and cross train cybersecurity talent already in your organisation.
- Identify potential new talent (or rule out unsuitable candidates)
- Benchmark performance against industry frameworks including MITRE, NIST, & OWASP

Education Seminars

Red Sift

Lessons from the dark side?

Rois Ni Thuama, Head of Cybersecurity Governance & Legal Partnerships, Red Sift

Fraud & prevention: Lessons in trust and identity

During this session, Red Sift's Head of Cyber Governance, Dr Rois Ni Thuama will:

- Explore a series of high-profile frauds that hit the headlines and look at what happened in each case
- Unpick the common denominators that bind these apparently diverse frauds
- Identify what organisations can learn from these fraudsters to shape and inform the steps they take to protect their firm's identity and reputation

RiskIQ

Using internet reconnaissance data to defend against targeted attacks

Vijay Punja, Technical Account Manager, RiskIQ

Network security monitoring solutions regularly highlight indicators associated to assets residing on the internet. Threat intelligence reports regularly detail threat actors and their tactics along with details of some of their assets. However, in both cases these indications are hosted on infrastructure that is connected to other adversary owned infrastructure. The challenge for most security teams is how to quickly assess what they are dealing with so they can take appropriate action. It's not enough to take defensive action against one or a group of URLs or IP addresses when that is only a small part of what could hurt you. You need to know what else those assets are connected to – in other words, the entire bad neighbourhood.

Because hackers can't avoid interacting with core components of the internet, they leave a trail of breadcrumbs over time; registered domains and certificates, servers and supporting infrastructure, fake websites and fishing pages, and campaign assets such as emails, social posts and SMSs that direct victims to their malicious assets. Fortunately, there are organisations like RiskIQ that monitor and map changes to the infrastructure of the internet over time to create global internet datasets that threat hunters can use to connect the dots to map out adversary infrastructure.

In this session we'll cover:

- What are internet datasets and how arethey created?
- What are the different types of internet datasets available and their specific strengths?
- What is infrastructure chaining and how can multiple internet datasets support this technique?
- How can your security researchers freely access internet datasets?

RiskIQ

Defending your organisation against JavaScript injection attacks

Terry Bishop, VP, Technical Services, RiskIQ

Browser-based attacks – web skimming, cryptocurrency miners, fingerprinters, and waterholing (including exploitation) encounters – are responsible for some of the most high-profile breaches in recent history, such as the hacks of British Airways and Ticketmaster. Given the frequency by which RiskIQ researchers now encounter these attacks, we believe that they should be taken as seriously as threat mainstays such as phishing and ransomware.

Browser-based attacks have one thing in common: malicious injects. These can be notoriously difficult to detect as their actions take place in the user's browser. The result is weeks or months of compromise on average.

In this session, we'll break down the most common and interesting injection techniques RiskIQ researchers have observed in our telemetry. We'll also look at ways organisations can defend themselves against this growing class of attack.

- JavaScript injection attacks – what are they?
- A brief history
- The current landscape – attackers acting with impunity
- Steps to defend against JavaScript injection attacks
- How RiskIQ can help

Education Seminars	
Swimlane **SOAR in the age of DX** **Toby Van de Grift,** UK Regional Director, Swimlane	Digital transformation impacts every part of a business: product creation, customer service, finance, time to market, time to value – everything is faster, more responsive and more 'granular'. So how does security exist in this new world, and what does this mean for Security Orchestration, Automation and Response (SOAR)? When correctly deployed, SOAR is truly transformative. It starts by simply augmenting humans in a linear workflow – getting more out of existing tech and your investment in staff. It can quickly evolve into a much higher value security tool. Swimlane has been automating and transforming SOCs since 2014 and we would like to share our knowledge and experience with you. My presentation will discuss: • What is the value of SOAR, and how do you harness it? • How does SOAR drive DX? • Why should you use SOAR and what factors should you consider?
Synack **Using hackers to beat hackers: innovation at Just Eat** **Justin Shaw-Gray,** Account Director, Synack Inc., and **Kevin Fielder,** CISO, Just Eat	There are big dilemmas in today's complex cybersecurity world. Year on year increases in cyber-attacks, an increase in the sophistication of these attacks, a widening cybersecurity talent gap – not to mention IT security budgets that haven't kept up with growing demands. And these are just some of the security issues companies face today. In this session, Synack's Justin Shaw-Gray will host an open conversation with Kevin Fielder, CISO, Just Eat. Justin and Kevin will discuss an innovative crowdsourced security model deployed at Just Eat and how Just Eat has ultimately made their platform a safer place for their customers. Attendees will learn how Just Eat: • Is using an army of ethical hackers to harden corporate assets • Has transformed and simplified security operations • Reduced the costs of legacy testing programs • And is now quickly deploying safer applications
TrapX Security **Building an effective deception strategy** **Nathan Gilks,** Regional Solutions Architect, TrapX Security	The TrapX platform allows you to deploy your company's deception strategy by using several layers of capability. Mask your entire network infrastructure by using a 'deception full stack' model. And emulate real network assets at scale without the need to deploy complex and costly systems or overburdening your critical resources. During our session, you will: • Understand why organisations are adopting a deception strategy • Walk-through the 'deception full stack' model • See a live demonstration of TrapX • Watch how easily deception traps can be deployed with little to no impact on resources • Realise how a scalable deception strategy can be implemented • Finally, delve into the rich ecosystem of security integrations demonstrating the value of TrapX working with your existing security defences to alert, respond and remediate
Tripwire **The future is hybrid: key considerations for cloud and DevOps** **Dean Ferrando,** Lead Systems Engineer, Tripwire	The elasticity and short lifespan of servers, paired with the up-and-coming wave of containerisation, introduces unique challenges to securing cloud infrastructure. In this session, we explore the key considerations and best practices for expanding security operations to the cloud and DevOps, including: • Understanding the responsibilities and controls of a hybrid environment • How to properly manage configuration and vulnerability risks • How to build trust across multiple cloud solution providers • And learn from the case study of a majorfinancial institution that successfully secured its hybrid enterprise

Education Seminars	
Wandera **Redefining the edge: making the most of your security investments a zero-trust world** **Adam Boynton,** Sales Manager, Wandera	Your employees work remotely. Your data is in the cloud. You've invested in solutions to help make users productive but with hackers targeting your endpoints, how do you keep your data – and your users – safe? It's time to redefine the enterprise perimeter. Join this session to discover: • Why legacy security architectures don't pay off • The evolving threats targeting your employees • Why user behaviour has changed and how to adapt • How to maximise your existing security investments • Three tips to avoid being the next Jeff Bezos (don't get hacked)
Zscaler **How you can achieve a zero trust network access** **Danny Phillips,** Senior Manager of Systems Engineering, Zscaler	Network-centric security wasn't built to secure the agile world of the cloud, which is why Gartner recommends embracing zero trust network access (ZTNA) technologies. ZTNA, also known as SDP, enables secure access to private apps across hybrid and multi-cloud environments enabling secure cloud adoption. Learn how ZTNA can help you obtain a zero trust access model whilst simplifying the management of not only your users, your controls, but also your access to applications. • How you can transform your network from open access to a secure, policy-driven framework • How to gain visibility of application access in a multi-cloud environment • Keeping your users secure, no matter where they are or how they are connected • Hide internal services from potentially malicious internet users