Post event report

Strategic sponsors

BITSIGHT The Standard in SECURITY RATINGS
Blue Cube Intelligent Protection
CROWDSTRIKE
CybelAngel
DEEP SECURE
Fidelis Cybersecurity
Gigamon
illumio
imperva
NETACEA
NTT Security
OneTrust Privacy Management Software
SECURE DATA TRUSTED CYBERSECURITY EXPERTS
SHAPE
wandera

Education Seminar Sponsors

activereach
AGARI
ANOMALI
Check Point SOFTWARE TECHNOLOGIES LTD.
DEMISTO
digital shadows
ecs security
GARRISON
INTEL471
INTSIGHTS Threat Intelligence Realized.
KENNA Security
McAfee Together is power.
NOMINET
PALISCOPE
Silobreaker
splunk>
Synack
ThreatMetrix A LexisNexis® Risk Solutions Company
Trustwave
VadeSecure Predictive Email Defense
ZoneFox A FORTINET COMPANY

Networking Sponsors

IDECSI Enterprise Security
REVERSING LABS
ThreatConnect
yubico

Branding Sponsor

Pulse Secure

> “The e-Crime & Cybersecurity Congress events always stand out from other security events, providing a somewhat unique combination of pertinent and relevant main-hall seminar sessions, coupled with a choice of educational seminars throughout the day. In addition, the venue is ideally placed to provide a good cross section of vendors and provide all the facilities needed at an event such as this, where like-minded professionals can network. Often at e-Crime & Cybersecurity Congress events I can make those important contacts with industry peers as well as speak to more vendors in one place than I could otherwise, making these events well worth the time out of the office. Thought-provoking, up-to-date and valuable.”
>
> **Group Info Sec Manager, WM Housing Group**

> “The event was great. The speakers and presentations were of very high standard compared to other events I have attended. The networking was above and beyond with so many companies and positions. The venue was in a great location and provided excellent catering for everyone to enjoy. I will recommend other security colleagues to attend in the future.”
>
> **Security Architect Specialist, AIB**

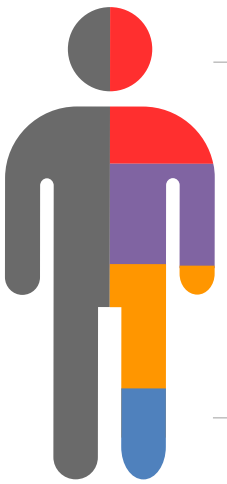
> “The e-Crime Congress enables us to evaluate where we are as an organisation in relation to unfolding events. We are very conscious that our exposure is limited and that we can easily get out of step with the trends taking place in cybersecurity. We have gained great value from real life experiences, learning from others and the issues they faced. In the past event, with representatives from law enforcement and legal professionals were extremely useful. The event is also invaluable in providing a platform to meet other practitioners to share experiences and ideas that you simply cannot get elsewhere. I have managed to get several of my colleagues coming to these events and they all have quickly realised that the e-Crime Congress delivers so much more than other similar events. The breadth of topics covered and the technical level of detail provided is invaluable.”
>
> **Senior cybersecurity Response Analyst, Canada life**

Inside this report:

Key themes

- Prepare for transparency now
- Cybersecurity: a core risk management discipline
- Third-party security: the weakest link?
- Innovation and security: allies or enemies?
- Running before you can walk
- Improving lives through smart communities and cities

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

Ashraf Aboukass, Global Head of Information Security Architecture, Schroders; Ryan Adams, Head of Financial Crime Intelligence, Aviva; Tony Adams, Head of Forensics, Digital Investigations and Prevent, NCA; Nick Baglin, General Manager, Netacea; Adrian Belcher, GSI Solution Architect EMEA, Gigamon; Sean Bennett, Strategic Account Director, EMEA, Shape Security; Stewart Bertram, Director of Professional Service and Closed Sources, Digital Shadows; Simon Black, Sales Engineer EMEA, Kenna Security; Patrick Boismenu, Head of Cyber-programme, UN Office on Drugs and Crime; Thomas Briend, Pre-Sales Engineer, Vade Secure; Paul Brucciani, Head of Commercial Business Development, Garrison Technology; Vineet Chhibber, Executive Director, ESG, JP Morgan Asset Management; Mohsin Choudhury, UK Head of Information Security, Bank of Ireland; Eddy Donald, former Global Chief Digital Risk Officer, VMLY&R; Ken Ducatel, Director, DG DIGIT, European Commission; Simon Edwards, Solutions Architect, Nominet; Khadir Fayaz, VP, Security Architecture and Engineering, Pearson; Tim Freestone, Principal Solutions Architect, Deep Secure; Phil Gaskell, Cybersecurity Specialist, Blue Cube Security; Tony Gaskin, Head of Information Security and Audit, Paragon Customer Communications; David Gray, Senior Manager & Practice Lead, NTT Security; Thomas Hallett, Privacy Solutions Engineer, OneTrust; Joseph Harris, Director of Intelligence Collection Management, Intel 471; Nigel Hawthorn, EMEA Marketing Director, McAfee; Lovisa Högberg, Head of Business Development, Paliscope; Dave Horton, Solutions Engineering Manager EMEA, OneTrust; Morgan Jay, Area Vice President, Northern EMEA, Imperva; Lynsey Jenkins, Director of Marketing, Fortinet; Mark Jones, CISO, Allen & Overy; Tom Kendrick, European Customer Success Manager, Check Point Software Technologies; Yara Khallouf, Cybersecurity Analyst Team Manager, CybelAngel; Muktadir Khan, Security Architect, Trustwave; Neil King, Business Information Security and Risk Specialist, Canon; Richard Kirk, Vice President EMEA, Illumio; James Linton, Lead Researcher, Agari; Jamie Lockhart, Sr. Solutions Engineer, Shape Security; Lloyd McAllister, Responsible Investment Analyst, Newton Investment Management; Harry McLaren, Managing Consultant, ECS Security; Aaron Mulgrew, Pre-Sales Consultant, Deep Secure; James Musk, Business Development & Sales Director, Trustwave; Mike Nathan, Senior Director – Solution Consulting EMEA (Head of Pre-Sales), ThreatMetrix; Ewen O'Brien, VP EMEA Sales, BitSight; Michael Owen, Head of Systems Engineering UK&I, IntSights
Danny Pickens, Director of Threat Research, Fidelis Cybersecurity; Ian Pitfield, Senior Technical Consultant, Netacea; Daniel Poole, Senior Security Solutions Engineer, Gigamon; Tom Plumer, Account Manager, Wandera; Chris Procter, Group Data Protection Officer, Whitbread; Peter Purwin, Director of Global Security Operations, Virgin Media; Raza Rizvi,Technical Director, activereach; Stephen Roostan, Regional Sales Director EMEA, Kenna Security; Suzan Sakarya, Sales Director, UK&I, Wandera; Tarun Samtani, Group Data Protection Officer, Boden Group; Reena Shah, Head of Information Security Culture and Awareness, M&G Prudential; Justin Shaw-Gray, Account Director, Synack Inc.; Dave Sheridan, Global Chief Information Security Officer, Santander
Pete Shorney, Global Head of Information Security, Rentokil; Nuno Silva, Consulting Engineer, BitSight; Martin Sivorn, Head of Cybersecurity, Government Digital Service; James Stevenson, Sales Director – UK, Nordics and Benelux, Demisto; Ian Thornton-Trump, Head of Cyber Security, AmTrust International; John Titmus, Director, EMEA, CrowdStrike; Charl van der Walt, Chief Security Strategy Officer, SecureData; Klas Waldenfors, Co-Founder and Marketing Manager, Paliscope; Robert Walker, Managing Director & Head of EMEA Asset Stewardship, State Street Global Advisors; Sally Webmark-Taylor, Head of Financial Crime Risk Name Screening, Aviva; Dave Whitelegg, Group Cyber Intelligence and Risk Officer, Capita

Agenda | Day 1 | 5th March 2019

08:00 Breakfast networking and registration

08:50 Chairman's welcome

09:00 **The dark underbelly of AML and fraud**

Sally Webmark-Taylor, Head of Financial Crime Risk Name Screening, Aviva, and **Ryan Adams,** Head of Financial Crime Intelligence, Aviva
- Insurance fraud – beyond crash for cash
- Using insurance companies for financial crime and money laundering
- What are Aviva doing to combat financial crime?

09:20 **The new wave of AI/ML cyber-attacks**

Ashraf Aboukass, Global Head of Information Security Architecture, Schroders
- What can emerging technologies such as artificial intelligence do to help security initiatives – and what new challenges do they introduce?
- Developing strategy and oversight of hyperconnectivity
- How are the cybercriminals using ML and AI techniques. What do information security leaders need to know to stay ahead of the game?

09:40 **A privacy playbook for 'reasonable and appropriate' security measures and safeguards**

Dave Horton, Solutions Engineering Manager EMEA, OneTrust
- Understand the requirements and importance of implementing 'reasonable and appropriate' security measures and safeguards for privacy professionals
- Outline several areas of common ground that should help every organisation align their security and privacy operations
- Take away a playbook for building a harmonised and risk-based security framework

10:00 **Transforming your defences**

Tim Freestone, Principal Solutions Architect, Deep Secure
- Appreciate the types of detection-based defences
- Understand the limitations of detection and why a new approach is needed
- Discover transformation and how it can be used to move beyond detection

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

Blue Cube Security	**Cyber solutions maturity framework – a pragmatic approach to information security** **Phil Gaskell,** Cybersecurity Specialist, Blue Cube Security
CrowdStrike	**Threat hunting: going into hand-to-hand combat with an advanced attacker** **John Titmus,** Director, EMEA, CrowdStrike
Illumio	**Yet another data breach?** **Richard Kirk,** Vice President EMEA, Illumio
Fidelis Cybersecurity	**How to apply threat intelligence to different real-world examples** **Danny Pickens,** Director of Threat Research, Fidelis Cybersecurity
Synack	**Innovation at Santander: using hackers to beat hackers** **Justin Shaw-Gray,** Account Director, Synack Inc. and **Dave Sheridan,** Global Chief Information Security Officer, Santander
ThreatMetrix	**Harnessing the power of a Digital Identity Network: reducing e-crime, building trust** **Mike Nathan,** Senior Director – Solution Consulting EMEA (Head of Pre-Sales), ThreatMetrix
Vade Secure	**Multi-phased attacks: the 1–2 punch that can knock your business cold** **Thomas Briend,** Pre-Sales Engineer, Vade Secure

11:00 Networking and refreshments

11:30 **Cyber-economics: information security metrics and incentives**

Martin Sivorn, Head of Cybersecurity, Government Digital Service
- Why information security needs metrics
- The use of data to inform decisions and measure progress
- Case study: security risk scores. A way of simplifying security risk into a numerical index that helped people understand the impact of new issues or mitigations
- The financialisation of cyber: incentives for security standards

11:50 **Security ≠ Friction**

Sean Bennett, Strategic Account Director, EMEA, Shape Security, and **Jamie Lockhart,** Sr. Solutions Engineer, Shape Security
Understand and defeat automated bot attacks whilst improving real user experience
- How have automated attacks evolved to defeat traditional security measures?
- Critical business impacts – what does this mean for you?
- Neutralising the threat: learn how to detect and mitigate even the most advanced automated attacks

12:10 **Not becoming the next cybersecurity headline is difficult, very difficult!**

Charl van der Walt, Chief Security Strategy Officer, SecureData
- The only certainty in cybersecurity is that high-profile compromises will continue to dominate the headlines. This leaves boards with the question: How do we prevent ourselves becoming the next headline?
- Most companies know that they need to implement a threat detection programme to get in front of the cyber-challenge. Getting it right is hard, very hard
- This talk looks at the overall threat landscape and provides a recipe for designing a threat detection programme whether you decide to outsource or do it yourself
- Key takeaways from this talk include understanding the building blocks and processes required to make sure you stand a chance of not becoming the next headline

12:30 **Device-centric security strategies for the modern work place**

Suzan Sakarya, Sales Director, UK&I, Wandera
- Mobile devices generate more corporate traffic than a traditional laptop or PC and traditional security investments such as SWG and EPP are no longer enough
- Many enterprise are looking to unify their mobile and traditional devices under one Unified Endpoint Management (UEM strategy)
- This is the perfect opportunity for companies to rethink their workspace security strategy and benefit from device-centric technologies such as MTD, CASB and Mobile SWG that are better suited to mobile deployment models
- In this session, Wandera will share best practices to help you design a device-centric security strategy for the modern workplace

Agenda | Day 1 | 5th March 2019

12:50	**Education Seminars | Session 2**	
	Agari	**Understanding the criminal mind: how Western European BEC syndicates leverage business intelligence** **James Linton,** Lead Researcher, Agari
	BitSight	**Avoid the cyber-risk blind spots in your supply chain** **Nuno Silva,** Consulting Engineer, BitSight
	Check Point	**How to protect the modern business from the weakest link** **Tom Kendrick,** European Customer Success Manager, Check Point Software Technologies
	IntSights	**The digital risk dilemma: how to protect what you don't control** **Michael Owen,** Head of Systems Engineering UK&I, IntSights
	Netacea	**Inside the mind of a cybercriminal: how to beat the bots** **Ian Pitfield,** Senior Technical Consultant, Netacea
	Trustwave	**Protect data and reduce risk with early detection & response services (MDRe) from Trustwave** **James Musk,** Business Development & Sales Director, Trustwave, and **Muktadir Khan,** Security Architect, Trustwave
	ZoneFox	**Harnessing UEBA and machine learning technologies to protect enterprises from insider threats** **Lynsey Jenkins,** Director of Marketing, Fortinet
13:30	Lunch and networking	
14:30	**EXECUTIVE PANEL DISCUSSION**	**Cloud: not such a fluffy concept. Key threats and costs of business efficient cloud security**
	Neil King, Business Information Security and Risk Specialist, Canon **Peter Purwin,** Director of Global Security Operations, Virgin Media **Chris Procter,** Group Data Protection Officer, Whitbread	
14:50	**Determining the important incidents**	
	Adrian Belcher, GSI Solution Architect EMEA, Gigamon • The industry is overwhelmed with security incidents and, with ever more alerts and limited expertise and budget, where do you start? • Adrian will take you through his customer experiences and how to resolve this • Discuss how, by stop doing perimeter security, you can start doing pervasive security • How you can stop buying security tools and start managing security tool lifecycles	
15:10	**Changing old thinking about operational technology to manage new risks**	
	David Gray, Senior Manager & Practice Lead, NTT Security • How are organisations establishing and assessing the internet of risk within their operational technology landscape? • What impact can the right threat intelligence make to detect and disrupt OT attacks? • Why forensic analysis really matters for long-term OT resilience	
15:30	**Education Seminars | Session 3**	
	Demisto	**Security Orchestration, Automation and Response (SOAR)** **James Stevenson,** Sales Director – UK, Nordics and Benelux, Demisto
	ECS Security	**Unleash the hunters** **Harry McLaren,** Managing Consultant, ECS Security
	Kenna Security	**Why visualising and reducing cyber-risk is a big data problem** **Stephen Roostan,** Regional Sales Director EMEA, Kenna Security, and **Simon Black,** Sales Engineer EMEA, Kenna Security
	Nominet	**DNS: One of cybersecurity's best kept secrets for eliminating network threats** **Simon Edwards,** Solutions Architect, Nominet
	Paliscope	**Move your online investigations forward with Paliscope** **Klas Waldenfors,** Co-Founder and Marketing Manager, Paliscope, and **Lovisa Högberg,** Head of Business Development, Paliscope
16:10	Networking and refreshments	
16:30	**Beyond the basics: emerging cyber-risks in the age of digital transformation**	
	Ken Ducatel, Director, DG DIGIT, European Commission • The rapid evolution of cyber-risks associated to both an enlargement of the attack surface and a fast changing threat landscape • The new risks of digital transformation: Cloud, mobile, social media, big data and AI are all providing new ways for avenues for attack • Meeting the challenges of digital transformation with specific reference to protecting an environment that is moving into cloud and which is increasing its use of big data and artificial intelligence	
16:50	**EXECUTIVE PANEL DISCUSSION**	**The peaks and pitfalls of impending AI and automation**
	Mark Jones, CISO, Allen & Overy (Chairman) **Tarun Samtani,** Group Data Protection Officer, Boden Group **Khadir Fayaz,** VP, Security Architecture and Engineering, Pearson	
17:10	**The changing nature of your crown jewels: what are your real vulnerabilities and how do you protect them?**	
	Mohsin Choudhury, UK Head of Information Security, Bank of Ireland • The changing nature of the crown jewels: is today's obsession with data and breaches the right way to think about businesses' cyber dependencies? What are the real weak links and how to protect them? • The relationship between fraud teams and cybersecurity teams • Recent breaches • Recommendations	
17:30	Networking and drinks reception	
18:30	End of day 1	

Agenda | Day 2 | 6th March 2019

08:00 Breakfast networking and registration

08:50 Chairman's welcome

09:00 **Prevent activity in cybercrime: a different approach**

Tony Adams, Head of Forensics, Digital Investigations and Prevent, NCA
- Cybercrime as a service: lowering the barrier to entry
- Cybercrime criminal pathways
- Positive diversions: Industry opportunities

09:20 **Combatting today's advanced attacker: key trends, predictions and the need for speed**

John Titmus, Director, EMEA, CrowdStrike
- LEARN FROM real-world examples of how cybercriminals combine advanced, targeted attack techniques with ransomware to cause massive financial loss
- GAIN INSIGHT into global 'breakout time' metrics and achieving the '1-10-60' rule to defeat adversaries and prevent a mega-breach
- PREPARE FOR THE NOW: discover the favourite tactics, techniques and procedures (TTPs) seen over the last 12 months to predict what you should expect to see in 2019

09:40 **Understanding the methods of intelligence**

Danny Pickens, Director of Threat Research, Fidelis Cybersecurity
- Define threat intelligence
- Make it consumable through requirements
- Acting on received intelligence

10:00 **Cyber gameplay: Strategic vs. Tactical thinking**

Ian Thornton-Trump, Head of Cyber Security, AmTrust International
- Securing hyper-connectivity. If you are just joining the hyper-connectivity race you are doomed to failure
- 5 key areas to focus on when it comes to cloud security
- The CFO as the most important stakeholder. Cyber as a business enabler
- The politics of cybersecurity

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

activereach	**DDoS on the frontline: how three large customers prepared for (and failed) a DDoS attack** **Raza Rizvi,** Technical Director, activereach
Digital Shadows	**Cyber-criminality beyond the Dark Web** **Stewart Bertram,** Director of Professional Service and Closed Sources, Digital Shadows
Garrison	**Defending yourself in a failing cybersecurity market** **Paul Brucciani,** Head of Commercial Business Development, Garrison Technology
Intel 471	**The rise of infostealers – what are they and why should I care** **Joseph Harris,** Director of Intelligence Collection Management, Intel 471
McAfee	**Cloud security – 50 shades of grey** **Nigel Hawthorn,** EMEA Marketing Director, McAfee

11:00 Networking and refreshments

11:30 EXECUTIVE PANEL DISCUSSION **The good governance of cyber: investors' truths on how they're rating the cybersecurity of your organisation**

Robert Walker, Managing Director & Head of EMEA Asset Stewardship, State Street Global Advisors
Lloyd McAllister, Responsible Investment Analyst, Newton Investment Management
Vineet Chhibber, Executive Director, ESG, JP Morgan Asset Management

11:50 **Transforming cybersecurity risk management, monitoring & reporting**

Ewen O'Brien, VP EMEA Sales, BitSight
- Prioritisation, justification and validation of IT security investments to underpin business digital transformation
- Managing third and fourth party risk in today's hyper-connected environment
- Supporting audit and compliance tracking including GDPR

12:10 **The credential craze: how to protect yourself from bots**

Nick Baglin, General Manager, Netacea
- How do you identify a bot from a human, and what can you do to stop the malicious ones from launching an account takeover attack?
- The rising sophistication of bots, the true extent of the problem and why it's everybody's problem
- Discover the approaches to mitigating the threat, when a new way is needed to outsmart the most sophisticated of bots

12:30 **Protect your digital crown jewels**

Richard Kirk, Vice President EMEA, Illumio
- Companies of all sizes are struggling to ensure that their network is truly secure using aging firewall security systems
- Micro-segmentation, when implemented correctly, can give them the security that they need and provide tremendous network visibility in the process
- Join us to learn what micro-segmentation is, how it works, and how to implement it

Agenda | Day 2 | 6th March 2019

12:50 Education Seminars | Session 5

Deep Secure	**Detection is dead** **Aaron Mulgrew,** Pre-Sales Consultant, Deep Secure
Gigamon	**How to streamline your security operations & incident response and gain visibility into encrypted traffic** **Daniel Poole,** Senior Security Solutions Engineer, Gigamon
OneTrust	**Risky business: a privacy & security team's guide to risk scoring** **Thomas Hallett,** Privacy Solutions Engineer, OneTrust
Shape Security	**Navigating the automated threat landscape: be sure you're protected from bot attacks** **Sean Bennett,** Strategic Account Director, EMEA, Shape Security, and **Jamie Lockhart,** Sr. Solutions Engineer, Shape Security
Trustwave	**Protect data and reduce risk with early detection & response services (MDRe) from Trustwave** **James Musk,** Business Development & Sales Director, Trustwave, and **Muktadir Khan,** Security Architect, Trustwave
Wandera	**The anatomy of a multi-layered mobile attack** **Tom Plumer,** Account Manager, Wandera

13:30 Lunch and networking

14:30 Bridging the business gap: uncovering cybersecurity as a corporate risk

Pete Shorney, Global Head of Information Security, Rentokil
- Cybersecurity is no longer just a technology issue, it's a business one too
- CISOs must communicate cyber-risk as corporate risk in order to get buy in from the board
- How does a CISO bridge the gap and partner with the business to build an effective risk management programme?

14:50 A lesson in aviation: the connected storage blind spot

Yara Khallouf, Cybersecurity Analyst Team Manager, CybelAngel
- Airports have become increasingly data-driven
- Data leaks have now become a critical threat to airport security
- An abundance of sensitive information, even that concerning airport security, circulates through connected devices
- Future IT ecosystem: connected storage and third parties

15:10 Why develop a financial risk assessment for data? How to translate and quantify the financial impact of your security investments and using that to drive the business case

Morgan Jay, Area Vice President, Northern EMEA, Imperva
A CISO sits on an average of 140 different types of software solving their security problems. How many of them can they say, hand on heart, bring actual value to the business?
- How can a business translate/quantify the financial impact of security investments and use that to drive a business case?
- How can a business help to solve the business problem proactively, thus making the right decisions for the right purchases strategically?
- How much would a business save if it focused on meaningful protection and alerts which can be truly and fully investigated?

15:30 Networking and refreshments

15:50 EXECUTIVE PANEL DISCUSSION What's happening to your business? Cloud security, new business metrics and future risks and priorities for 2019 and beyond

Dave Whitelegg, Group Cyber Intelligence and Risk Officer, Capita
Eddy Donald, former Global Chief Digital Risk Officer, VMLY&R
Tony Gaskin, Head of Information Security and Audit, Paragon Customer Communications

16:10 Real-world stuff. International truths on cyber CNI

Patrick Boismenu, Head of Cyber-programme, UN Office on Drugs and Crime
- Real world examples. Not strategies and methodologies
- The real issues with legislation, retaining data and digital forensics
- What are the criminals using?
- Cryptocurrency and real world criminality

16:30 Moving past cybersecurity training and awareness as a tickbox exercise

Reena Shah, Head of Information Security Culture and Awareness, M&G Prudential
- Moving past cybersecurity training and awareness as a tickbox exercise. Can senior management use training as a way of ticking a box rather than actually investing in the much more expensive and difficult process of truly managing cybersecurity? How do you evolve security culture past this so it is a critical part of business infrastructure?
- How to engage board members and get investment. Get the metrics and prove the ROI of security awareness and training
- Case study from one of the largest teams and budgets dedicated to information security training

16:50 Closing remarks

17:00 Congress close

Education Seminars

activereach

DDoS on the frontline: how three large customers prepared for (and failed) a DDoS attack

Raza Rizvi, Technical Director, activereach

Large and destructive DDoS attacks against major businesses are now commonplace. As a DDoS testing provider, it is our job to demonstrate how easy it is to break through mitigation defences and bring down internet facing systems – albeit within a controlled, safe environment. Our experience evidences a staggering 85% of organisations are unable to mitigate a DDoS attack, even with enterprise-level mitigation in place.

Join us to hear how three major institutions – from the finance, utilities and e-commerce sectors – failed the test. We reveal the security gaps in their mitigation defences and share best practice in DDoS testing & preparation for a DDoS attack.

What attendees will learn:

- The most common DDoS mitigation oversights & how to avoid them
- How to identify and eliminate any single points of failure in your company's infrastructure, including those with third parties
- How to develop a human response plan for addressing attacks when they arise including best practice for running DDoS drills
- How to model your risk when different parts of your infrastructure are liable to attack
- Actionable guidance for your own DDoS attack response plan

Agari

Understanding the criminal mind: how Western European BEC syndicates leverage business intelligence

James Linton, Lead Researcher, Agari

Please join James Linton, Lead Research Intelligence at Agari as he exposes the inner workings of a sophisticated, UK-based cybercriminal organisation. Learn the tactics of this group, how they leveraged business intelligence to iprofile their targets on which they launched their Business Emails Compromise attacks.

This session will shed light on:

- The inner-working of BEC criminal groups
- What responsible active defence techniques can we use to identify and disrupt cybercriminal organisations
- How can we combat a cybercriminal that operates like a modern corporation?

BitSight

Avoid the cyber-risk blind spots in your supply chain

Nuno Silva, Consulting Engineer, BitSight

Participants will see a live view into the BitSight Portal. We will demonstrate how continuous cyber-risk monitoring works for your company and the affiliates, your suppliers and peers.

What will attendees learn:

- Insight into the riskiest issues impacting your vendors
- Confidence to make faster, more strategic decisions on cyber-risk management
- Launching and scaling up your TPRM with the resources you have today

Blue Cube Security

Cyber solutions maturity framework – a pragmatic approach to information security

Phil Gaskell, Cybersecurity Specialist, Blue Cube Security

Technology is built and maintained by generalists but in depth cybersecurity needs specialist knowledge to offer the protection businesses needs in today's world of ever-increasing risks.

Join our specialist cybersecurity consultant from solution provider Blue Cube Security's services team, Cynergy. Our aim is to highlight any gaps in your security infrastructure and help you understand how these can be filled.

What attendees will learn:

- Risk quantification and your maturity in the world of cybersecurity
- How to reduce unknown unknowns
- Enlighten you as to the correct future investment in security and technology
- Help you maximise the return on investment for the products you have purchased and exploiting their full potential

Education Seminars	
Check Point Software Technologies **How to protect the modern business from the weakest link** **Tom Kendrick,** European Customer Success Manager, Check Point Software Technologies	Cyber-attacks are more dangerous than ever before, and with malicious toolkits out in the wild, the barrier to entry is very low! With tools and techniques available to hackers that focus on compromising the user, how does Check Point, the world leading security vendor, help your users stay protected? We will look at: • How protecting all attack surfaces is now a must • Some simple tools and techniques available to the hackers • How machine learning and AI engines can predict the next attack
CrowdStrike **Threat hunting: going into hand-to-hand combat with an advanced attacker** **John Titmus,** Director, EMEA, CrowdStrike	Ever wonder how the hackers get in, or what they do once they have infiltrated a network? Learn about the latest attack techniques that have been uncovered by CrowdStrike's threat hunting and incident response teams including: initial attack vectors, persistence, lateral movement and data exfiltration techniques. Using examples of real-world attacks, we outline the critical steps of defence and proactive threat hunting that must occur if companies are to aggressively seek out sophisticated threat behaviours that elude even the best automated security systems. • Using real examples, see how cybercriminals combine advanced, targeted attack techniques with ransomware to achieve massive financial payoffs via 'Big Game Hunting' • Find out how you can stop these and other types of attacks before they start and what you can do to prevent a malware-free intrusion • Understand how threat hunting can be used to identify and stop advanced attacks in your environment, and how to defend your organisation against advanced attacks
Deep Secure **Detection is dead** **Aaron Mulgrew,** Pre-Sales Consultant, Deep Secure	• Attackers have evolved to using continually changing automated attacks against financial services and critical national infrastructure • Current defences, including detection-based technologies' mantra of 'detect and respond' isn't enough to cope with the sophisticated tools that the modern hacker has access to • How to evade detection. Demonstrating how to evade detection in practice with real-world malware samples • How to cope with the document based threat. What you can do about the document based threat to your organisation
Demisto **Security Orchestration, Automation and Response (SOAR)** **James Stevenson,** Sales Director – UK, Nordics and Benelux, Demisto	Accelerating incident response, while ensuring a consistent process every time. By 2021, 70% of all SOCs will deploy security automation capabilities, up from less than 5% in 2018. This high rate of adoption is driven by increasing alert volumes impacting the triage process, a security skills gap in the market, and the need to accelerate incident response to reduce the window of exposure and associated business risk. This workshop will cover the key business challenges driving the rapidly emerging SOAR market (Security Orchestration, Automation and Response), and demonstrate how you can automate repetitive, costly and time consuming tasks with playbooks, enabling you to scale anything from IOC enrichment to malware analysis and phishing investigations.
Digital Shadows **Cyber-criminality beyond the Dark Web** **Stewart Bertram,** Director of Professional Service and Closed Sources, Digital Shadows	The Dark Web has historically been viewed by many cybersecurity professionals as a nexus for online criminality. Mainstream media coverage around high-profile sites such as The Silk Road having highlighted the overt criminality of the Dark Web. However, these stories often miss out the sense of community and trust that binds cyber-criminal underground together. This talk examines this point and more in an effort to more fully understand online cyber-criminality and how it is practised. Point that are covered include: • What role Dark Web communities play within the cyber-criminal kill chain • How the Dark Web may expand in the future • What draws people to online criminality and what keeps them within that community

Education Seminars	
ECS Security **Unleash the hunters** **Harry McLaren,** Managing Consultant, ECS Security	Reduce the burden on your valuable security analysts and maximise the use of their time by re-evaluating the objectives, priorities and processes of your security operations centre. Ensure your analysts have the tools and resources they need to hunt effectively and enable them to protect your organisation by looking for and identifying real and present threats to deliver more effective risk management. Traditional approaches to threat detection have proven to be ineffective; often producing low-value incidents and analyst fatigue through high ratios of false positives. Modern threat hunting and risk reduction should be well planned, structured and orchestrated to make best use of the technologies and people that exist within your organisation. This session will give you an insight into how we approach threat hunting with a focus on effective planning, use of technology and analyst empowerment. Unleash the hunters! You will learn: • Threat hunting best practice recommendations • How to empower your SOC to find unknown threats • How to support hunters via agile platforms • How to mitigate the risk of rapid change to your SIEM
Fidelis Cybersecurity **How to apply threat intelligence to different real-world examples** **Danny Pickens,** Director of Threat Research, Fidelis Cybersecurity	The use of intelligence continues to mature within cybersecurity. Adopting a proven model will assist in making intelligence applicable at every organisation. This seminar will cover how intelligence can be adopted and consumed beyond typical indicators of compromise feed ingestion to mature an organisation's capability and lead to applying intelligence through a decision making process. What attendees will learn: • A basic understanding of the threat intelligence lifecycle • How to apply threat intelligence to different real-world examples • Integrating threat intelligence in a threat model framework • Open source resources that can be used to study and mature an understanding of applied threat intelligence
Garrison **Defending yourself in a failing cybersecurity market** **Paul Brucciani,** Head of Commercial Business Development, Garrison Technology	We are the online generation. We spend more time online than we do asleep. The problem is that the internet was designed 40 years ago in a completely different threat landscape, without today's security needs in mind. Cyber-attacks today are more frequent, widespread and damaging than ever before. Despite spending $114bn in 2018, cybersecurity doesn't feel like a battle we are winning. Boards are pressuring CISOs and CSOs to find better ways to protect us that cost less. The founders of Garrison recognised that this is too big a problem to fix with current cyber controls and set out to build a solution that could help large businesses to take a significant leap ahead. We returned to basics, and noticed that the common theme in the vast majority of attacks is the corporate internet link – it's the route used in the vast majority of attacks to get in and cause harm. And so we created Garrison to fundamentally fix this key vulnerability. Delegates attending the seminar will learn: • How to overcome the barriers to IT security: IT complexity; vendor mistrust; and disincentives to innovation • How enterprises are applying security techniques used by security agencies to eliminate web browsing risk and to restore secure internet access to knowledge workers • How Garrison has combined these techniques with hardware innovation in a product that isolates web threats from trusted assets in a way that is highly assured

Education Seminars	
Gigamon **How to streamline your security operations & incident response and gain visibility into encrypted traffic** **Daniel Poole,** Senior Security Solutions Engineer, Gigamon	Learn how you can streamline your Security Operations Centre team and provide swifter responses to security incidents by having actionable data for each event available to your security teams as events unfold. In this session, we also discuss how to gain visibility into encrypted traffic coming into and leaving your environment, thereby mitigating data exfiltration and APT threats from and to your organisation. You will learn: • How to provide visibility into encrypted traffic • How to leverage the knowledge and expertise of seasoned security professionals to immediately improve your security posture • How to increase the reach of your tools and increase the life and effectiveness of your security countermeasures • How to spot the tell-tale signs of stolen credentials being used for nefarious purposes
Illumio **Yet another data breach?** **Richard Kirk,** Vice President EMEA, Illumio	Have you ever wondered why hacks and data breaches keep on happening? With the average time before discovery of over 200 days, it is inevitable that a breach will happen. In this session you will: • Learn about how hackers take advantage of your network • Understand what you are looking for • Gain some tips on how to make their lives difficult
IntSights **The digital risk dilemma: how to protect what you don't control** **Michael Owen,** Head of Systems Engineering UK&I, IntSights	More of your attack surface resides on web infrastructure you don't own or control. To protect your digital assets and prevent malicious lookalikes on everything from social networks to criminal marketplaces, you must shift security priorities from prevention to detection and remediation. This session will outline tools, tactics and best practices to safeguard your entire digital footprint. • Monitor the clear, deep and dark web for your organisation's digital assets • Gain visibility and take action when malicious brand lookalikes pop-up • Discover and mitigate phishing attacks targeting your executives and customers
Intel 471 **The rise of infostealers – what are they and why should I care** **Joseph Harris,** Director of Intelligence Collection Management, Intel 471	Since the end of 2018, Intel 471 has observed a substantial increase in the production and use of Info Stealer malware and the trading of data gathered by these tools. Join us for a session as we explore in much more detail recent insights into this activity and demonstrate how threat actors are utilising the data harvested with malicious intent. Through this session you can learn how to get one step ahead of malicious actors and minimise risk of impact to your organisation and third party suppliers as a result of the practical advice and guidance offered.

Kenna Security
 	
Why visualising and reducing cyber-risk is a big data problem
 	
Stephen Roostan, Regional Sales Director EMEA, Kenna Security, and
Simon Black, Sales Engineer EMEA, Kenna Security
	Join Kenna Security for a discussion on how architecting big data at scale, married to data science algorithms through the lens of cyber-risk, can very quickly enable multiple value streams across an organisation – addressing the common goals of risk reduction and improved cybersecurity posture.
	
	We will cover:
	
	• Are you really vulnerable to an open vulnerability?
	• The results of marrying data science to threat intelligence on a huge scale, quickly.
	• Champions in the enterprise:
	  ○ The power of technical partnership
	  ○ Visualising risk to the board
	  ○ Normalising the view of risk across multiple business units/tools
	  ○ How to enable ITOps/DevOps to be part of the remediation task force

Education Seminars

McAfee

Cloud security – 50 shades of grey

Nigel Hawthorn, EMEA Marketing Director, McAfee

This is a business risk. Not an IT risk. Security systems can be complex to implement, however some of them are at least easy to explain – malware is always bad and some websites are always inappropriate for business. Cloud is different and we need to come from a different angle. The volume of data that business deal with on a daily basis has become unmanageable. For many organisations, moving critical data to the Cloud is the only feasible business option, but, as one major retail CISO said, "when you move to the Cloud, you forgo a certain element of control". 72% of business have faith that data stored in the Cloud is actually more secure than when it is stored on-premise. But shared responsibility, and poor visibility are just a few of the risks that have raised the security stakes.

The pressure is higher than ever on the information security leader to work with a Cloud security provider that they trust, who understands content, context and user behaviour to ensure appropriate policies. Some cloud services may be high risk, but even low risk services can be used in a high-risk manner. In this education seminar, McAfee will be drawing on real-life case studies and sharing unique insights on how Cloud security is impacting the CISO's role, and the policies, procedures and partnerships they need to get it right.

In this session, attendees will learn:

- From real-life case studies how leading organisations successfully integrated Cloud security to address their key business priorities
- Hard hitting truths about Cloud security risks. What in your organisation is most vulnerable and what you need to do
- How to make a case for a comprehensive cloud adoption team to address cloud needs
- The threat of insider threat. The greatest data loss made through the Cloud is by people just trying to get their jobs done. What are the solutions?
- Everything is about reducing risk. High-level lessons in Cloud security risk management
- Ten examples to think about and take back to your office the next day

Netacea

Inside the mind of a cybercriminal: how to beat the bots

Ian Pitfield, Senior Technical Consultant, Netacea

With the complexity and number of botnets and account takeover attacks increasing, we take you on a whistle stop tour of the threat landscape and demonstrate how easy it is for cybercriminals to target your website. We will discuss some of the tool, tactics and procedures used by cybercriminals and take a practical look at the different approaches to dealing with an increasingly complex threat landscape. We also discuss the perfect storm faced by organisations in the wake of massive data breaches as they battle to strike the balance between account security and the end user experience.

Attendees will gain practical insights into:

- How attackers can access stolen credentials
- What tools and techniques attackers commonly leverage
- Different approaches to dealing with the bot activities and their limitations
- Questions to ask when evaluating bot management solutions

Education Seminars

Nominet

DNS: One of cybersecurity's best kept secrets for eliminating network threats

Simon Edwards, Solutions Architect, Nominet

The growth of cyber-threats and growth of data are fast creating significant problems for businesses. There's too much information and not enough action, as stretched resources try to keep networks secure, while coping with the demands of digital transformation and regulatory compliance. It's not just the known threats you need to worry about; some of the biggest headaches come from trying to stay ahead of criminal developers. Whilst there are many solutions available as part of the security stack, the value of DNS as a critical source of information to check for threats and monitor the health of a network is often overlooked. Learn why understanding your DNS traffic is vital to your security visibility and how advanced techniques can be applied to predict, detect & block threats before they harm your network.

What attendees will learn:

- The overload facing IS/IT professionals
- How and why DNS is such vital part of networks and the internet and an often-exploited mechanism
- Applying advanced analytic techniques to DNS traffic can turn it into an advantage – predicting, detecting and blocking threats – known and unknown
- How this analysis is highly complementary to existing tools and can be used to enrich SIEM information, cutting the window of compromise and contributing to reducing the compliance workload
- How proactive monitoring can help contextualise a network so that anomalous behaviour acts as an early indicator of threats

OneTrust

Risky business: a privacy & security team's guide to risk scoring

Thomas Hallett, Privacy Solutions Engineer, OneTrust

Risk scoring across vendor management, breach notifications, DPIAs and other activities is imperative for compliance with many global privacy laws and security frameworks. Organisations routinely tailor their data protection and security activities based on the results of detailed risk assessments, but this leads to a myriad of questions. How do you calculate risk? What constitutes low, medium or high risk? How do you define a risk criteria? What's the difference between inherent, current and residual risk? In this session, we'll detail the importance of conducting risk assessments under global privacy laws like the GDPR and security frameworks such as ISO 27001, provide scenario-based approaches to risk assessment and give examples on how to tailor your approaches based on risk level.

- Understand various approaches to conducting risk assessments
- Learn how to define a risk criteria and how to calculate risk level
- Learn how to tailor your privacy and security programmes using a risk-based approach

Paliscope

Move your online investigations forward with Paliscope

Klas Waldenfors, Co-Founder and Marketing Manager, Paliscope, and
Lovisa Högberg, Head of Business Development, Paliscope

Today, people share more information online than ever before. This is something that we can make use of when conducting an online investigation. With Paliscope, investigators can quickly and easily collect open source data for review and analysis, sort and prioritise among the collected data, connect correlating intelligence to find more clues, and create professional reports to share the results with other parties.

Used by law enforcement agencies, insurance companies and the finance sector, Paliscope helps investigators to tackle all sorts of cases online. No matter if it is a case of investigating an insurance fraud, doing background checks in a recruitment process or monitoring cyber-threats – you can always be helped by searching the internet for information about a subject's online presence and digital footprints.

What attendees will learn:

- How to start an investigation from scratch; developing a small piece of information into a full case of intelligence
- How to gather online information in a structured and secure way, verifying how and where the data was collected to be able to prove its validity
- How Paliscope together with integrated online services can be used to search for more clues online
- How to generate professional reports and keep third parties informed along the investigation process

Education Seminars	
Shape Security **Navigating the automated threat landscape: be sure you're protected from bot attacks** **Sean Bennett,** Strategic Account Director, EMEA, Shape Security, and **Jamie Lockhart,** Sr. Solutions Engineer, Shape Security	Security is no longer just about inadvertent vulnerabilities. Attackers are abusing application functionality to conduct automated and manual fraud. These fraudsters will continue to evolve for as long as they are able to extract value from your application. • Recognise the evolution of automated threats • Understand how automated attacks affect different verticals, including gaming, finance and retail • Discuss critical business impacts • Neutralising the threat: evaluate advanced detection and mitigation methods
Synack **Innovation at Santander: using hackers to beat hackers** **Justin Shaw-Gray,** Account Director, Synack Inc., and **Dave Sheridan,** Global Chief Information Security Officer, Santander	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 difficulties companies face today. In this session, Synack's Justin Shaw-Gray will host an open conversation with Dave Sheridan, Global Chief Information Security Officer for Santander Corporate & Investment Banking. Justin and Dave will discuss an innovative crowdsourced security model deployed at Santander and how Santander has ultimately made the bank a safer place for their customers. Attendees will learn how Santander: • Utilised an army of ethical hackers to harden corporate assets • Transformed and simplified security operations • Reduced the costs of legacy testing programmes • And quickly deployed safer applications
ThreatMetrix **Harnessing the power of a Digital Identity Network: reducing e-crime, building trust** **Mike Nathan,** Senior Director – Solution Consulting EMEA (Head of Pre-Sales), ThreatMetrix	Digital businesses continue to walk a tightrope of balancing online friction with effective fraud control. Fraudsters are masquerading as good customers using stolen identity credentials, recruiting customers as unwitting accomplices to advanced social engineering attacks, and using mass-scale networked bot attacks to cripple business defences. Yet customers expect streamlined and frictionless access to goods and services without unnecessary intervention. Join this presentation to hear: • How harnessing a global view of trust, and risk, helps detect and block advanced fraud • Building trust using digital identity intelligence can help better distinguish between good customers and fraudsters in near real time • An analysis of recent attack patterns and fraud typologies from the ThreatMetrix Digital Identity Network, which analyses 110 million transactions a day • Examples of live fraud attacks including detecting and blocking mule networks across the banking ecosystem.

Education Seminars

Trustwave

Protect data and reduce risk with early detection & response services (MDRe) from Trustwave

James Musk, Business Development & Sales Director, Trustwave, and
Muktadir Khan, Security Architect, Trustwave

Is your business struggling to detect advanced threats?

Typically, detection is only visible months after a compromise or breach and by then, just how much damage has been caused to your business?

When leaving attackers to move undetected throughout your systems, you're increasing the risk of unfounded damage and/or loss during such breaches. This can be avoided with Trustwave's pro-active managed threat hunting, powered by Trustwave Managed Detection & Response for Endpoints (MDRe), delivered by Trustwave SpiderLabs. A recognised team of experts located across the company's global network of ASOCs who leverage behavioural analytics, multiple intelligence feeds for deep insights into potential, isolate malicious behaviour, remediate these threats proactively, and identify other potential threats that may be present in your environment.

During our education session, you will learn why:

- Detecting attacks early lies in fully leveraging pro-active threat hunting
- Managed Threat Detection service helps identify cloud and on-premise threats earlier based on security information and event management solutions
- MDRe from Trustwave correlates additional data to leverage security events from combined technologies, enabling recurring threat investigation and remediation

Trustwave brings innovative Managed Security Services that is putting businesses back in the driver's seat when it comes to threat detection and response

Vade Secure

Multi-phased attacks: the 1–2 punch that can knock your business cold

Thomas Briend, Pre-Sales Engineer, Vade Secure

Heading into 2019, the volume – and sophistication – of email threats is growing. Phishing is virtually indistinguishable from legitimate brand communications, spear phishing is hyper-personalised using publicly available data, and insider attacks are surging due to the popularity of cloud email services. But the biggest danger of all is when cybercriminals combine these vectors in multi-phased attacks.

Gain insight into how multi-phased attacks are designed and how your business can prevent being knocked cold by one. We'll use data and real-world examples to highlight the massive growth in Office 365 phishing, and show you how cybercriminals use compromised accounts to launch spear phishing, malware, and insider attacks. The goal is never the credentials themselves but rather a financial payout in the form of wire transfers, ransoms, or access to proprietary information.

Gain insight into:

- How cybercriminals execute coordinated, multi-phased attacks
- Why Office 365 is the most targeted entry point
- How data breaches are jet fuel for targeted email attacks

Wandera

The anatomy of a multi-layered mobile attack

Tom Plumer, Account Manager, Wandera

Gartner predicts that 1/3 of all malware will be on mobile by 2019. Yet traditional security methods aren't up to the task of protecting your mobile fleet and hackers are often three steps ahead. As mobile threats look to target the user themselves with SMS phishing attacks or hotspot spoofing, it is imperative that IT teams understand what the attackers are trying to accomplish so the appropriate defence can be mounted.

In this talk, we will deconstruct a mobile attack to demonstrate how cybercriminals are gaining a foothold on modern mobile devices.

- Explore the top mobile threats that compromise your company data
- Discover why zero-day protection is the only way to target this new breed of cyber-threats
- Delve into the motivations behind attackers and the techniques being used to trick your employees
- Experience a live hack and how this can be tailored to verticals for maximum impact

Education Seminars	
ZoneFox **Harnessing UEBA and machine learning technologies to protect enterprises from insider threats** **Lynsey Jenkins,** Director of Marketing, Fortinet	Cybersecurity trends come and go, but machine learning looks to be here to stay. According to McAfee, 43% of data breaches in recent years were caused by employees, contractors or suppliers, either negligently or maliciously. How can we harness UEBA and machine learning technologies to protect against the insider threat? What attendees will learn: • What the insider threat looks like in 2019 • Where UEBA and machine learning fit into the cybersecurity landscape • Getting started with UEBA technology – the challenges and considerations • What it means for the security team