Post event report

e-crime & cybersecurity CONGRESS

The 16th e-Crime & Cybersecurity Congress

6th & 7th March 2018 | London, UK

Strategic sponsors

Bitdefender

Centrify THE BREACH STOPS HERE

COFENSE

CROWDSTRIKE

DARKTRACE

DEEP SECURE

IMPERVA

InteliSecure

Menlo Security IT'S SAFE TO CLICK

MICRO FOCUS

NTT Security

SECURE DATA TRUSTED CYBERSECURITY EXPERTS

TESSIAN

wombat security technologies

ZoneFox

Education Seminar Sponsors

AGARI

ANOMALI

BITSIGHT The Standard in SECURITY RATINGS

CYBERBIT PROTECTING A NEW DIMENSION

DUO

egress

EyeOn ID

foreseeti

GROUP IB

KENNA Security

Malwarebytes

SAI GLOBAL

Skyhigh

TITUS

TREND MICRO

Networking Sponsors

THREATCONNECT

XQ CYBER

> “I'd like to thank you for allowing me to attend. I learnt some good things from the vendors, which were my reasons for attending, i.e. to learn and understand what security products may/may not help our organisation.”
>
> **IT Security Manager, BTL Group Ltd**

> “This was the 2nd year I attended the e-Crime & Cybersecurity Congress and I would not miss it again. It's a brilliant forum for getting some perspective around your security posture whilst being able to appreciate we all have the same common enemy and goals.”
>
> **IT Director, SevenC3**

> “The Congress overall was excellent, with a wide range of topics being covered. I was particularly impressed with the presentations on the second day and the topics that were covered, from Michael Stawasz at the US Dept of Justice covering hack back – and why we should do it – to the view portrayed by fund investors given by David Sneyd, and for the presentation skils (as well as the content) of the presentation by Simon Wiseman.”
>
> **Head of IT Audit, Crossrail TFL**

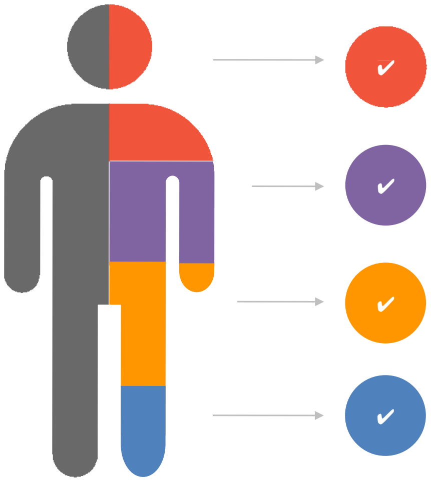
> “The e-Crime & Cybersecurity Congress is one event that I try not to miss. The topics presented are relevant and of good standard. The event is also excellent for networking with people from different industries/sectors and gaining knowledge from peers and vendors.”
>
> **IT Security & Risk Officer, UBS**

Inside this report:

Key themes

- Securing CNI
- Securing the IoT
- The government response to cyber-threats
- International law enforcement co-operation
- Collaboration between the public and private sectors
- Accountability for cybersecurity as a business risk

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

Charles Arthur, former Technology Editor, The Guardian; Marcella Atzori, Blockchain Advisor & GovTech Expert; Nigel Brown, Lead for Resilient ICT Strategy, Civil Contingencies Secretariat, Cabinet Office; Don Chadwick, Technical Account Manager, TITUS; Michael Colao, CISO, AXA; Mischa Danaceau, Chief Information Security Officer, InteliSecure; Kevin Davis, Chief Investigator, Serious Fraud Office; Ben Dickinson, Founder and Managing Director, 3VRM; David Doherty, Global IM Cyber GRC specialist, Anglo American; Malcolm Dowden, Legal Director, Womble Bond Dickinson; Paul Down, Senior Director, EMEA, Wombat Security Technologies; Philip East, UK Sales Director, BitSight Technologies; Anthony Eskander, Barrister, KPMG, Legal Services; Nathan Gilks, Solutions Director, Deep Secure; Etienne Greeff, Chief Technical Officer and Founder, SecureData; Henk Grootveld, Fund Manager and Head of Trends Investing Equity Team, Robeco; Sam Hampton-Smith, Head of Engineering, ZoneFox; Nigel Hawthorn, EMEA & Privacy Spokesperson, Skyhigh Networks/McAfee; Jacob Henricson, Senior Risk Management Advisor, foreseeti AB; Mollie Holleman, Senior Intelligence Specialist, Cofense; Mike Hulett, Head of Operations, National Cyber Crime Unit (NCCU); Helge Husemann, Global Technical Evangelist, Malwarebytes; Len Hynds, CSO, Modern Times Group; David Janson, VP Sales, UK & Europe, Cofense; Morgan Jay, Area Vice President for the UK & Northern Europe, Imperva; Simon Jenner, Chief Information Security Officer, Booking.com; Paula Kershaw, Regional Head of Cybersecurity, Europe and UK, HSBC; Peter Lee, Principal Security Engineer, Imperva; Emma Leith, Head of Digital Security & Risk/CISO, Corporate Functions and Trading, BP; Jeff Lenton, Technical Lead EMEA, Kenna Security; Niall MacLeod, Sales Engineering Director, EMEA, Anomali; William J. Malik, VP Infrastructure Strategies, Trend Micro; Sam Martin, Senior Cybersecurity Manager, Darktrace; Kelly McCann, UK Sales Director, Egress Software Technologies; Scott Mellis, Cybercrime Liaison Officer to the UK, Australian Federal Police; Gary Miles, Detective Chief Inspector, Operation FALCON, Metropolitan Police; Nic Miller, former CISO, Brevan Howard, virtual CISO; Jonathan Morgan, European Director, Agari; Michael Moshiri, Senior Director of Product Marketing, Duo Security; Laurentiu Popescu, Global Senior Manager, Marketing Research, Insights & Intelligence, Bitdefender; Liam Puleo, Sales Engineer, Bitdefender; Helen Rabe, CISO, CBRE; Brett Raybould, Solutions Architect, Menlo Security; Stuart Reed, Senior Director – Market Strategy, NTT Security; Tony Rowan, Lead Solutions Engineer, Cyberbit; Anna Russell, Head of Data Security Consulting, Micro Focus; Justine Sacarello, Head of Legal and Regulatory Change, Group Transformation, Lloyds Banking Group; Abhirukt Sapru, Head of Business Development, Tessian; Barry Scott, CTO, EMEA, Centrify; Michael Sentonas, Vice President, Technology Strategy, CrowdStrike; Imran Sheaikh, Vice President Cyber Risk, Barclays; Kev Smith, Systems Engineer, Centrify; David Sneyd, Senior Associate, Governance & Sustainable Investment, BMO Global Asset Management; Daniel Söderberg, CEO, Eyeonid Group; Michael Stawasz, Head of the Cybersecurity Unit and Deputy Chief for Computer Crime, US Department of Justice; Thom Thavenius, Deputy CEO, Eyeonid Group; Henry Trevelyan Thomas, Head of Client Development, Tessian; Zeki Turedi, Cyber Security Expert, CrowdStrike; Sudeep Venkatesh, Chief Product Officer, Egress Software Technologies; Charl van der Walt, Chief Strategy Officer, SecureData; Dmitry Volkov, Head of Threat Intelligence, Co-founder, Group-IB; Simon Wilkes, European Director, SAI Global; Simon Wiseman, Chief Technology Officer, Deep Secure

Agenda | Day 1 | 6th March 2018

08:00 Registration and breakfast networking

08:50 Opening remarks

09:00 **Law enforcement and industry: Partnership to protect**

Mike Hulett, Head of Operations, National Cyber Crime Unit (NCCU)

- The changing face of the enemy: Why cyber-attacks are becoming more frequent and more sophisticated
- Success stories from NCCU. Our strategy for protecting businesses and CNI
- Why collaboration is key. Why is there still such a huge problem with reporting of cybercrime?
- How can law enforcement and industry work towards a more transparent relationship

09:10 **Ransomware: Its past, present and future**

Michael Colao, CISO, AXA

- The fundamental truth about ransomware: The evolution of nation-state tools and the need for effective risk modelling
- Ransomware as a multi-million dollar business, and why the big corporates don't pay
- Why board members are under attack – and need to be engaged

09:40 **State of the Phish 2018: What your peers are doing to reduce successful phishing attacks**

Paul Down, Senior Director, EMEA, Wombat Security Technologies

- Aggregation and analysis of data from tens of millions of simulated phishing attacks sent through Wombat's Security Education Platform over a 12-month period
- Responses from quarterly surveys of Wombat's, as well as data from an international survey of working adults who were queried about social engineering threats and their cybersecurity behaviours
- Insights into current vulnerabilities, industry-specific phishing metrics, and emerging threats

10:00 **Security as a Service (SECaaS): Cybersecurity in the Cloud age**

Stuart Reed, Senior Director – Market Strategy, NTT Security

- Mobile, IoT, and Cloud-based workloads are increasingly leading to complex digital environments that need securing
- Stretched budgets and resources mean security leaders are looking for alternatives to traditional cybersecurity management
- SECaaS is gaining popularity in the Cloud age, but what should organisations be considering when moving their security solutions to the Cloud?

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

Anomali	**Building an effective threat intelligence programme** **Niall MacLeod,** Sales Engineering Director, EMEA, Anomali
Egress Software Technologies	**Please delete my previous email** **Kelly McCann,** UK Sales Director, Egress Software Technologies
Eyeonid Group	**How to protect your business against credential stuffing attacks** **Daniel Söderberg,** CEO, Eyeonid Group; and **Thom Thavenius,** Deputy CEO, Eyeonid Group
foreseeti AB	**Threat modelling: The challenge in managing risk of both structural and technical vulnerabilities** **Jacob Henricson,** Senior Risk Management Advisor, foreseeti AB
Kenna Security	**Predict where cyber-attackers will strike next** **Jeff Lenton,** Technical Lead EMEA, Kenna Security
SAI Global	**Your third parties may be placing bets you're not willing to make!** **Simon Wilkes,** European Director, SAI Global
Trend Micro	**Strategies for securing three classes of IoT** **William J. Malik,** VP Infrastructure Strategies, Trend Micro
Wombat Security Technologies	**Turning end-user security into a game you can win** **Paul Down,** Senior Director, EMEA, Wombat Security Technologies

11:00 Networking and refreshment break

11:30 **The growing cost of behaviour-enabled cybercrime**

Paula Kershaw, Regional Head of Cybersecurity, Europe and UK, HSBC

Learn from one of the largest global financial institutions who should take responsibility for cybersecurity and how to get senior management to treat cybersecurity as a real business issue.

- With the growing cost of cybercrime, why is cybersecurity still not recognised as a business issue?
- How we can educate and support our people to both protect themselves and our organisations
- Who is accountable for the cybersecurity in your organisation? How should we be changing the way we think about cyber-risk?

11:50 **A new era of cyber-threats: The shift to self learning, self defending networks**

Sam Martin, Senior Cybersecurity Manager, Darktrace

- Leveraging machine learning and AI algorithms to defend against advanced, never-seen-before, cyber-threats
- How new immune system technologies enable you to pre-empt emerging threats and reduce incident response time
- How to achieve 100% visibility of your entire business including Cloud, network and IoT environments
- Why automation and autonomous response is enabling security teams to neutralise in-progress attacks, prioritise resources, and tangibly lower risk
- Real-world examples of subtle, unknown threats that routinely bypass traditional controls

12:10 **Overcome on-premise restrictions, seamlessly and consistently securing your Cloud workloads when migrating to hybrid IT**

Anna Russell, Head of Data Security Consulting, Micro Focus

- Focus on how businesses are consistently looking to migrate to hybrid IT architectures to respond to today's business drivers for speed and agility and how launching secure Cloud applications is a critical enabler to accelerate this
- Learn how Micro Focus can help embed security within the data lifecycle, consistently and seamlessly across hybrid IT

12:30 **Zero Trust Security – never trust, always verify**

Barry Scott, CTO, EMEA, Centrify

Organisations spent a combined $170bn on cybersecurity in 2016 and 2017. During the same period, 66% of organisations experienced an average of five or more data breaches. A larger security budget simply won't solve the cybersecurity problem. An entirely new approach is required – Zero Trust Security. The benefits of Zero Trust Security are crucially important in this climate of ever increasing number and scope of security breaches. Zero Trust Security:

- Covers the broadest range of attack surfaces, ranging from users, endpoints, and networks to resources
- Enables organisations to increase business agility through the secure adoption of Cloud and mobile solutions
- Provides a framework to properly manage the risk of exposing sensitive apps and infrastructure to business partners
- Creates satisfied, productive users by ensuring the proper controls are in place to address appropriate levels of risk without requiring a heavy-handed, maximum-control approach regardless of the risk posed

Agenda | Day 1 | 6th March 2018

12:50	**Education Seminars | Session 2**	
	Agari	**How to combat email attacks and identity fraud** **Jonathan Morgan,** European Director, Agari
	Cyberbit	**Failing to plan is planning to fail: A perspective on cybersecurity training** **Tony Rowan,** Lead Solutions Engineer, Cyberbit
	Darktrace	**The future impact of AI in cybercrime** **Sam Martin,** Senior Cybersecurity Manager, Darktrace
	Group-IB	**Analysis of Cobalt attacks on financial institutions: SWIFT, processing, ATMs** **Dmitry Volkov,** Head of Threat Intelligence, Co-founder, Group-IB
	Malwarebytes	**Exploits in the cryptocurrency craze: What you must know to protect your organisation** **Helge Husemann,** Global Technical Evangelist, Malwarebytes
	SecureData	**Battlefield Earth 2018: It used to be security was a network thing** **Charl van der Walt,** Chief Strategy Officer, SecureData
	TITUS	**Oversharing and the Cloud generation. What will data protection look like in the future?** **Don Chadwick,** Technical Account Manager, TITUS
13:30	Lunch and networking	
14:30	**Cybersecurity: The investor's priority**	
	Henk Grootveld, Fund Manager and Head of Trends Investing Equity Team, Robeco • Truths from one of the largest global investors and asset managers • Cybersecurity as a risk indicator for investors • Cybersecurity as an investing opportunity • Combining risk and opportunities	
14:50	**A new era of cybersecurity**	
	Laurentiu Popescu, Global Senior Manager, Marketing Research, Insights & Intelligence, Bitdefender • Evolution of the security threats landscape • Security counter defence to elusive attacks • A shift in paradigm: The adaptive security framework • Data privacy and integrity in the centre of security practices	
15:10	**Cybersecurity in 2018: The impact of compliance regulation, threat intelligence and machine learning**	
	Sam Hampton-Smith, Head of Engineering, ZoneFox • What caught the headlines in 2017 – and what we can learn from them • How AI and machine learning are changing the security landscape • And why technology alone can't keep your data secure	
15:30	**Education Seminars | Session 3**	
	Bitdefender	**Disrupt the attack kill chain** **Liam Puleo,** Sales Engineer, Bitdefender
	Centrify	**Zero Trust Security in practice** **Barry Scott,** CTO, EMEA, Centrify; and **Kev Smith,** Systems Engineer, Centrify
	CrowdStrike	**Hacking exposed: Stories from the battlefield – lessons learnt in responding to the most advanced cyber-attacks** **Zeki Turedi,** Cyber Security Expert, CrowdStrike
	foreseeti AB	**Threat modelling: The challenge in managing risk of both structural and technical vulnerabilities** **Jacob Henricson,** Senior Risk Management Advisor, foreseeti AB
	ZoneFox	**What does the marriage of machine learning and cybersecurity look like in 2018?** **Sam Hampton-Smith,** Head of Engineering, ZoneFox
16:10	Networking and refreshment break	
16:30	**EXECUTIVE PANEL DISCUSSION**	**There's no such thing as cyber-risk...or is there?**
	Cybersecurity is now a recognised business issue. Good news, right? Or is it? In this executive panel discussion, hear how major business leaders have managed their cybersecurity risk and how they get the message across to thier senior management. Does cybersecurity risk actually exist, or is it all part of wider business risk? How do you provide clear metrics? Join this interactive panel discussion and find out. **David Doherty,** Global IM Cyber GRC specialist, Anglo American **Imran Sheiakh,** Vice President Cyber Risk, Barclays **Helen Rabe,** CISO, CBRE **Laurentiu Popescu,** Global Senior Manager, Marketing Research, Insights & Intelligence, Bitdefender **Chaired by Len Hynds,** CSO, Modern Times Group	
16:50	**Lions and sheep on the Dark Web**	
	Etienne Greeff, Chief Technical Officer and Founder, SecureData • Things that go bump in the night, what we fear, what we should fear, and how that affects what we do in security • Taking a look at some of the big lions we've been watching, who they've been catching and what that all means for us • Overview of today's landscape and key trends including: Innovation of monetisation by criminals; Industrialisation of offensive cyber-capabilities; and Legislation • How to address the real issues – that matter!	
17:10	**Cybersecurity – winning the great game**	
	Simon Jenner, Chief Information Security Officer, Booking.com • CISOs are now major players in the 'great game': How do you avoid the common pitfalls and how do you win? • What is at stake? Identify your core business assets and protect them from current threats • The impact of machine learning and AI on cybersecurity	
17:30	Drinks and networking	
18:30	End of Day 1	

Agenda | Day 2 | 7th March 2018

08:00 Registration and breakfast networking

08:50 Opening remarks

09:00 **The cyber-attacked hack back**

Michael Stawasz, Head of the Cybersecurity Unit and Deputy Chief for Computer Crime, US Department of Justice

- Hack back – the new idea everyone's talking about to secure your business. But is it all it seems?
- Proactive defence. What do you need to know? What are the advantages and risks?
- The US Department of Justice conclusion: Why hack back is counter-productive for cybersecurity

09:20 **The state of cyber: How stealthier attacks are blurring the lines between cybercrime and statecraft**

Michael Sentonas, Vice President, Technology Strategy, CrowdStrike

This session will shed light on alarming new trends CrowdStrike has observed in the global threat landscape, and the evolving best practices that are proving most successful against criminal, hacktivist and nation-state adversaries.

- The latest threat intel and predictions for 2018 and how you can use this to shape your security strategy
- 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 continue to succeed in evading modern defences
- How applied threat intelligence can deliver a decisive advantage in protecting your enterprise

09:40 **5 ways to strengthen your phishing defence programme for 2018**

David Janson, VP Sales, UK & Europe, Cofense

- Learn the best ways to introduce and communicate a programme, based on results of over 27 million end users across 160 countries
- Discuss tips for increasing engagement and building resiliency among your workforce
- Find out the most important metrics your Board and C-level Execs will want to review
- Discover how to handle repeat clickers and reduce end-user susceptibility by 95%

10:00 **Taking the UD out of FUD: Battling the fear, uncertainty and doubt in cybersecurity**

Emma Leith, Head of Digital Security & Risk/CISO, Corporate Functions and Trading, BP

Case study of a success story from one of the largest FTSE 100 multinationals.

- The success story of culture change. How cybersecurity was implemented as part of key business culture and strategy from a culture of fear. How is cyber now in fact a critical element to consider when it comes to issues of CNI?
- Getting board level engagement. How to get the key message across the senior management and communicate the real business impact of cyber-risk. Balancing the technical role and business engagement
- How to get cybersecurity investment. How to communicate the message that there is 'no silver bullet solution' while still maintaining the ROI and business value of investing in security protection

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

BitSight Technologies	**How to manage cyber-risk on a daily basis for your company and the affiliates, your suppliers and peers** **Philip East,** UK Sales Director, BitSight Technologies; and **Ben Dickinson,** Founder and Managing Director, 3VRM
Cofense	**2018 phishing trends: New year. New threats. Same dark intentions** **Mollie Holleman,** Senior Intelligence Specialist, Cofense
Duo Security	**Zero trust access: Five steps to securing the perimeter-less enterprise** **Michael Moshiri,** Senior Director of Product Marketing, Duo Security
InteliSecure	**Exploring preferential risk strategies for cybersecurity investments** **Mischa Danaceau,** Chief Information Security Officer, InteliSecure
Skyhigh Networks/ McAfee	**With Cloud, BYOD and remote working – how do you control your data?** **Nigel Hawthorn,** EMEA & Privacy Spokesperson, Skyhigh Networks/McAfee
Tessian	**What were the causes behind the biggest data breaches in 2017?** **Henry Trevelyan Thomas,** Head of Client Development, Tessian

11:00 Networking and refreshment break

11:30 **Paranoid and prudent: Questions and answers from your investors on cybersecurity risk**

David Sneyd, Senior Associate, Governance & Sustainable Investment, BMO Global Asset Management

- How does the cybersecurity of a company affect its investment value?
- What are investors looking for when assessing cyber-resilience?
- What questions do investors ask their investee companies? And why are these crucial to the CISO?

11:50 **Managing unquantifiable risk**

Simon Wiseman, Chief Technology Officer, Deep Secure

- Appreciate that malware detection leaves you with unquantifiable risk because it isn't fully effective
- Understand why unquantifiable risk is inevitable with common types of defence
- Realise that there is nothing inevitable about unquantifiable risk
- Discover how transformation can make cyber-risk management something definitive

12:10 **True cybercriminals are only after your data – why are we not defending against it?**

Morgan Jay, Area Vice President for the UK & Northern Europe, Imperva

- Cybercriminals ONLY monetise on data
- The threats are not just from the outside
- Database and applications are the biggest risk
- How to manage 'AOS' – 'Alert Overload Syndrome?'

Agenda | Day 2 | 7th March 2018

12:30	**Education Seminars | Session 5**	
	Agari	**How to combat email attacks and identity fraud** **Jonathan Morgan,** European Director, Agari
	Deep Secure	**Attackers are better at evasion than we are at detection … how do we break this cycle?** **Nathan Gilks,** Solutions Director, Deep Secure
	Egress Software Technologies	**Please delete my previous email** **Sudeep Venkatesh,** Chief Product Officer, Egress Software Technologies
	Eyeonid Group	**How to protect your business against credential stuffing attacks** **Daniel Söderberg,** CEO, Eyeonid Group; and **Thom Thavenius,** Deputy CEO, Eyeonid Group
	Imperva	**Alert and data overload! Using analytics and machine learning to simplify security in data protection** **Peter Lee,** Principal Security Engineer, Imperva
13:10	Lunch and networking	
14:10	EXECUTIVE PANEL DISCUSSION	**Let's not get cryptic about crypto** In this high-level, informal panel discussion, we will be uncovering the truths behind cryptocurrency, blockchain and developments in fintech. Everyone is talking about blockchain, but does anyone actually know anything about it? What are the changes blockchain will have on the way we operate and secure our businesses? Join us and our leading industry experts to find out. **Marcella Atzori,** Blockchain Advisor & GovTech Expert **Nic Miller,** former CISO, Brevan Howard, virtual CISO **Anthony Eskander,** Barrister, KPMG, Legal Services **Chaired by Charles Arthur,** former Technology Editor, The Guardian
14:30		**Convincing the business to fund critical cybersecurity initiatives** **Mischa Danaceau,** Chief Information Security Officer, InteliSecure • Communicating security concepts to non-technical audiences • Capitalising risks associated with data leakage • Cost benefit analysis for incremental cybersecurity investment
14:50		**Misaddressed emails were the biggest form of data loss in 2017** **Abhirukt Sapru,** Head of Business Development, Tessian • The risk that data loss poses to enterprises • The important role that reporting plays in understanding and minimising this risk • The various layers of accountability within every firm that inform how CISOs can make their firms more secure
15:10		**Isolation – your next best friend** **Brett Raybould,** Solutions Architect, Menlo Security • Spear-phishing is a top 3 security risk but detection & training do not stop successful attacks • Web browsers remain a major part of the attack surface but how can you balance access & security for all employees? • Tired of jumping every time there is Flash or IE 0 day exploit to patch? There's no need! • Learn how large global banks use remote browsing/isolation to protect employees from cyber-attacks
15:30	Refreshments and networking	
15:50		**Blockchain governance for highly sensitive data: Mitigating risks and e-crimes** **Marcella Atzori,** Blockchain Advisor & GovTech Expert Marcella Atzori will be sharing exclusive insights on blockchain technology, cryptocurrency, and its impact on our business operations. What will blockchain mean for your role? Gain lessons she has shared with governments, leading institutions, and academic communities. • Highly sensitive data: Improving security and resilience through DLTs and decentralised governance • What are the new risks and e-crimes emerging in the blockchain industry, and how can we mitigate them? • The blockchain eco-systems currently existing for highly sensitive data: How they work and why they are safer than others
16:10	EXECUTIVE PANEL DISCUSSION	**Laying down the (cyber) law** Industry and law enforcement need collaboration and compromise. We have brought together leaders in law enforcement from around the world to share international perspectives including: tackling cybercrime, the issues with disclosure, and what businesses need to do to protect themselves. **Nigel Brown,** Lead for Resilient ICT Strategy, Civil Contingencies Secretariat, Cabinet Office **Scott Mellis,** Cybercrime Liaison Officer to the UK, Australian Federal Police **Kevin Davis,** Chief Investigator, Serious Fraud Office **Gary Miles,** Detective Chief Inspector, Operation FALCON, Metropolitan Police
16:30	EXECUTIVE PANEL DISCUSSION	**How to manage the security of the third parties you work with** Every business has to work with third parties. You have an invested interest in knowing about their security. But how do you understand and measure it? What questions do you ask? Join two industry experts and understand: • The need for 'robust processes' in measuring and analysing the security of the third parties you work with • How to implement a system of metrics to value and measure cyber-risk • The effect that AI, machine learning and blockchain technology are having on business systems and infrastructure **Malcolm Dowden,** Legal Director, Womble Bond Dickinson **Justine Sacarello,** Head of Legal and Regulatory Change, Group Transformation, Lloyds Banking Group
16:50	Conference close	

Education Seminars	
Agari **How to combat email attacks and identity fraud** **Jonathan Morgan,** European Director, Agari	Email is the primary infiltration mechanism for the majority of cyber-attacks. To effectively combat these attacks, organisations need to understand the types of identity deception attackers typically prefer, the relative risk and cost of attacks to businesses and the likelihood of their success. What attendees will learn: • Explore the latest threat research into characteristics of known email-based cyber-attacks • Examine the prevalence of low-volume, socially engineered email attacks that easily bypass existing security layers • Quantify the relative risk and cost of attacks to your business • Understand how your enterprise can innovate to detect attacks using spear phishing and identity deception
Anomali **Building an effective threat intelligence programme** **Niall MacLeod,** Sales Engineering Director, EMEA, Anomali	This seminar will cover what goes into a good threat intelligence programme: where do I get data from, how should it be managed and how to use it effectively. We'll refer to the recent SANS 2018 Cyber Threat Intelligence Survey for background and we'll look at why implementing a threat intelligence platform (TIP) isn't the end of the process. Finally we'll cover a complimentary threat modelling methodology that focusses on the effects of a breach, not the causes. What attendees will learn: • Where to collect threat data from • Managing the relevance of threat data (internal and external) • Sharing threat data through ISACs or peer communities • Adding workflows around Anomali's threat intelligence platforms • Threat modelling with STRIDE-LM
Bitdefender **Disrupt the attack kill chain** **Liam Puleo,** Sales Engineer, Bitdefender	Using a layered approach to reduce the overall attack surface is standard practise but how do we protect against the recent trend of advanced attacks. Liam will discuss how more sophisticated attacks are being widely used with devastating consequences and demonstrate some techniques to mitigate the risk of impact to your business. What attendees will learn: • Advanced techniques malicious actors are using to compromise your organisation • 'File less' malware, script-based attacks and how they can be stopped • Hacking tools and exploit kits are tools an attacker can easily obtain. How to step up the game in protection • Live advanced attack demonstration
BitSight Technologies **How to manage cyber-risk on a daily basis for your company and the affiliates, your suppliers and peers (Live view in the BitSight Portal)** **Philip East,** UK Sales Director, BitSight Technologies; and **Ben Dickinson,** Founder and Managing Director, 3VRM	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 attendees will learn: • How the cyber-risk rating can be improved in the easiest way. All risk vectors and the results will be demonstrated • How cyber-risk for your own company and the affiliates, the suppliers and peers can be managed based on qualified events and ratings

Education Seminars	
Centrify **Zero Trust Security in practice** **Barry Scott,** CTO, EMEA, Centrify; and **Kev Smith,** Systems Engineer, Centrify	Practical examples of how your organisation can begin to adopt Zero Trust Security. What attendees will learn: How Zero Trust Security • Covers the broadest range of attack surfaces, ranging from users, endpoints, and networks to resources • Provides a framework to properly manage the risk of exposing sensitive apps and infrastructure to business partners • Improves the user experience by ensuring proper controls are in place to address appropriate levels of risk
Cofense **2018 phishing trends: New year. New threats. Same dark intentions** **Mollie Holleman,** Senior Intelligence Specialist, Cofense	Join Cofense for a look back at 2017's threats and a look ahead. We'll provide an overview of what our Cofense Intelligence team uncovered, discuss trends in phishing-delivered malware, and analyse how various delivery vectors evolved. What will attendees learn: • The implications of last year's major global cyber-events, such as WannaCry and NotPetya • The emergence of new ransomware families • The abuse of legitimate functions built into business-critical software platforms to deliver malware • The favouring of modularity and plug-in accompaniments to lightweight botnet and stealer malwares • New ways cybercriminals are obtaining cryptocurrency
CrowdStrike **Hacking exposed: Stories from the battlefield – lessons learnt in responding to the most advanced cyber-attacks** **Zeki Turedi,** Cyber Security Expert, CrowdStrike	CrowdStrike continues to expose unprecedented efforts by highly sophisticated adversaries targeting – and in some cases, selectively leaking – information stolen from sensitive government, corporate and private networks. These intrusions reflect a broad range of motives and targets, revealing many never-before-seen tactics, techniques and procedures (TTPs) that are advancing the art of data manipulation and attack obfuscation, while raising the bar significantly for organisations seeking to protect themselves from these potentially disruptive and destructive attacks. This session will shed light on alarming new trends CrowdStrike has observed in the global cyber-threat landscape, and the evolving best practices that are proving most successful against criminal, hacktivist and nation-state adversaries. What attendees will learn: • How nation-state threats are crafted and how their tactics, techniques and procedures (TTPs) are infiltrating the corporate world in the form of advanced attacks • Who are the most notable adversaries in 2018 and the key European security themes based on the latest threat intel report published by CrowdStrike's global intelligence operation • What are the indicators of attack and how you can apply them to defeat the adversary?

Education Seminars

Cyberbit

Failing to plan is planning to fail: A perspective on cybersecurity training

Tony Rowan, Lead Solutions Engineer, Cyberbit

In a world where the defender is often at a technical disadvantage and the personnel to form that defence team are in short supply, it is no wonder that headline grabbing cyber-attacks are common place. Without the ability to train personnel effectively with the knowledge, skills and practices needed to detect, investigate and respond to attacks, organisations are doomed to fall to the hands of the hackers.

The session looks at how current training mechanisms address the skills shortage in cyber-defenders and investigators and examines how to address the fundamental issues of repeatability, measurement and scale in various training systems.

What attendees will learn:

- What current thoughts are regarding the skills gap in cyber-defence
- How current training systems have evolved to attempt to address the skills gap
- The difficulties and deficiencies in those training systems
- How to improve training performance measurement and reporting
- How to create effective repeatable cyber-defence training
- How to maintain the efficiency and skills levels of trained personnel in the face of evolving attack techniques and tools

Darktrace

The future impact of AI in cybercrime

Sam Martin, Senior Cybersecurity Manager, Darktrace

What attendees will learn:

- How AI has a profound impact on our future inter-net, and the potential for it to enable digital criminals
- The complexity of business and protection, and how current defenders are being outpaced
- Machine learning and advanced mathematics as tools for handling complexity
- Real-life examples and applications of attacks
- Inevitable rise of data theft and how best to protect yourself

Deep Secure

Attackers are better at evasion than we are at detection … how do we break this cycle ?

Nathan Gilks, Solutions Director, Deep Secure

Join Deep Secure's Solutions Director, Nathan Gilks, in a session on why detecting cyber-threats will soon be a thing of the past. Everyone is facing more relentless, sophisticated and undetectable cyber-attacks – from polymorphic malware that's designed to fool security controls – to the rise of stegware (steganography attacks). All slipping right in and harvesting your crown jewels whilst hidden in plain sight…

What attendees will learn:

- Sophisticated attacks inbound that get easily evaded
- Going covert and leaking data out without DLP batting an eye lid
- How you can change the rules of the game – protection without detection!

Duo Security

Zero trust access: Five steps to securing the perimeter-less enterprise

Michael Moshiri, Senior Director of Product Marketing, Duo Security

The perimeter-based security approach of the last century is no longer adequate for securing the modern enterprise. Today, organisations must secure a mobile workforce that uses a mix of corporate-owned and personal devices to access Cloud-based applications and services, often from outside corporate networks. The zero trust access model delivers that security without cumbersome and antiquated technologies such as VPN and MDM.

What attendees will learn:

- How the zero trust access model works,
- How leading organisations such as Google use this approach to secure access to their critical applications and data
- How you can implement this model in your organisation in five logical steps

Education Seminars

Egress Software Technologies

Please delete my previous email

Kelly McCann, UK Sales Director, Egress Software Technologies

Whether or not we'll admit to having sent an Outlook recall or similar message, most of us will probably at least acknowledge that we've been on the receiving end of one. When emails are sent in error, the best-case scenario is that the sender is left a little red faced; at worst, however, it can allow unauthorised access to personal and corporate data. When this happens, an Outlook recall really isn't a good enough defence.

What's more, email isn't the only way your staff can share information with unauthorised recipients, both accidentally and maliciously. Yet for many organisations, it's a Catch 22: you need communication channels to be available for work processes yet in doing so, you expose your organisation to risk.

There is, however, another way. In this session, Egress will explore how organisations can use security technology to put users at the centre of this problem to find its solution. We'll look at how machine learning and AI can be used to engage with end users to ultimately drive adoption of security technology and reduce risk.

What attendees will learn:

- The real risk employees pose by sharing sensitive personal and corporate data with unauthorised recipients
- How machine learning and AI can be used to engage end users with security technology
- How organisations can prevent the 'accidental' (fat finger) email send
- That it is time to dispel the myth of 'Man vs Machine' and replace it with 'Man and Machine' if they are to effectively prevent future data breaches

Eyeonid Group

How to protect your business against credential stuffing attacks

Daniel Söderberg, CEO, Eyeonid Group; and **Thom Thavenius,** Deputy CEO, Eyeonid Group

Massive data breaches continue to make the news on a seemingly daily basis. But after every significant breach, a new threat lurks in the background.

Stolen credentials are traded on the Dark Web in their billions. Once acquired, these data sets are used by hackers to bombard third-party websites in credential stuffing attacks. If an unsuspecting account holder has used the same credentials compromised in a separate breach on a third-party site, the hackers can gain access and masquerade as legitimate users. Unfortunately, a culture of password reuse and the rise of massive data breaches mean in many cases these cybercriminals are successful.

After gaining access to an account, hackers have free reign to commit fraud, causing a great deal of disruption to both the user and the website owner.

These attacks damage a brand's reputation, and the clean-up can be very costly indeed.

Thankfully, by the end of this seminar, you will have discovered a new way to protect your site and your users from this kind of attack. A brand new, next-generation fraud detection platform that will tackle the hackers head on.

What attendees will learn:

- Why credential stuffing attacks are growing in size and frequency
- What happens when a hacker gains access to an account under the guise of a legitimate user
- How the fallout from a credential stuffing attack can decimate consumer confidence in a brand
- How a brand new credential validation platform can guard against such attacks

Education Seminars

foreseeti AB

Threat modelling: The challenge in managing risk of both structural and technical vulnerabilities

Jacob Henricson, Senior Risk Management Advisor, foreseeti AB

Companies today are experiencing an ever-increasing connectivity and complexity of infrastructure risk management. The underlying challenge today is that infrastructures are complex and interconnected, let alone the fact that a lot is run in the Cloud. With the complexity of architectures increasing, the focus on technical vulnerabilities is not enough. Traditional vulnerability scanning offers insight on technical vulnerabilities but lacks the ability to prioritise what to focus on.

That said, in general, there needs to be a more holistic approach to ensure that risk is managed in a proper way related to IT infrastructures. Using a combination of technical and structural vulnerabilities, being able to map large infrastructures in a scalable way, needs to be combined with a probabilistic approach in threat modelling, which enables organisations to focus on true risk instead of theoretical risk on a technical level.

Taking this further, and being able to focus on true business risk, requires a new approach. At the Royal Institute of Technology, extensive research has been conducted in threat modelling and the probability of a certain set of parameters to be exploited to get access to an infrastructure.

Join this seminar to learn the latest of research on threat modelling from both academia and the corporate world.

What attendees will learn:

- Distinction between technical and structural vulnerabilities
- How to address the challenges in scaling traditional risk assessments and threat modelling of complex IT infrastructures with objective fact-based data
- Using research findings to perform threat modelling on large corporate IT infrastructures
- How to use threat modelling in the design process of IT infrastructures

Group-IB

Analysis of Cobalt attacks on financial institutions: SWIFT, processing, ATMs

Dmitry Volkov, Head of Threat Intelligence, Co-founder, Group-IB

What attendees will learn:

- Evolution of Cobalt group TTPs – strategic & technical analysis
- What systems Cobalt target in banks and how thefts take place
- Analysis of joint operations between Cobalt and other financial APT actors

Imperva

Alert and data overload! Using analytics and machine learning to simplify security in data protection

Peter Lee, Principal Security Engineer, Imperva

Every day a new story about data loss is in the news. The primary security controls in most organisations focus on network and endpoint, yet networks are not stolen from the data centre and endpoints don't typically contain the massive data leaked. So why do traditional controls fail to address the primary theft target – data?

Security departments agree that they have too many alerts to effectively review, too few staff to manually support the technology solutions in place and are now being asked to increase their scope to include data protection into their responsibilities.

Join us for a live presentation on how you can leverage on analytics and machine learning to protect your data in a better way!

What attendees will learn:

- How to build an effective data security practice through the use of machine learning and analytics
- The new way to look at data and alert
- How to create security awareness and mitigation across your data landscape?
- Building the foundation for many technical requirements of GDPR and other regulations

Education Seminars	
InteliSecure **Exploring preferential risk strategies for cybersecurity investments** **Mischa Danaceau,** Chief Information Security Officer, InteliSecure	Join InteliSecure Chief Information Security Officer, Mischa Danaceau, for a hands-on workshop to explore the holistic foundations of assessing cybersecurity risk within your organisation, aligning appropriate models to overcome investment concerns for budget holders, and benchmarking against cybersecurity investment projection. What attendees will learn: • How to financially quantify cybersecurity risk • How to quantify benefits of risk-treatment strategies • How to calculate total cost of ownership for a security investment • How to deliver an ROI projection for a security proposal • Monitoring and evaluating performance of programme to projection
Kenna Security **Predict where cyber-attackers will strike next** **Jeff Lenton,** Technical Lead EMEA, Kenna Security	The latest exploit prediction capabilities are taking cyber-threat forecasting to a new level of accuracy and giving IT security teams a head start on preventing attacks. Jeff explains how machine learning, predictive modelling, and big data techniques can be used to provide powerful, actionable forecasts for organisations, based on their own assets and vulnerabilities. What attendees will learn: • Immediately evaluate new vulnerabilities to predict whether cyber-attackers will weaponise them • Calculate and assign risk score for prioritisation against all risks in the context of your own environment • Prioritise high-risk vulnerabilities, so you can allocate remediation resources efficiently • Evolve from reactive threat management to predictive risk management
Malwarebytes **Exploits in the cryptocurrency craze: What you must know to protect your organisation** **Helge Husemann,** Global Technical Evangelist, Malwarebytes	As long as cybercriminals can make a profit, businesses and their data will always be a target. However, this is just the beginning to the new attack vectors and threats organisations are now facing. Learn about a few of the trends and recent attack methods that our research labs have discovered pertaining to nefarious block-chaining and illegal drive-by crypto-mining. We will uncover how these attacks are being delivered and how your company or personal electronic devices may be at risk – without you even knowing it. Additionally, we will identify the essential security measures that your customers must incorporate to protect themselves and their company. What attendees will learn: • The current/future state of drive-by and crypto-mining within the cryptocurrency realm • TTPs (Techniques, Tactics, Procedures) used to assist in illegal block-chaining activities • Best of breed security practices needed to mitigate and protect yourself and your organisation from these new drive-by block-chaining attack vectors • Last but not least a couple of tips and things to think of if you are the CIO/CISO of an organisation from a 10-year old 'start up'

Education Seminars	
SAI Global **Your third parties may be placing bets you're not willing to make!** **Simon Wilkes,** European Director, SAI Global	With GDPR impacting global companies that hold data on European Union (EU) citizens, businesses are having to take immediate steps with regards to their outsourced processors to comply with this regulation. Third-party risk is a real and expansive threat. Some of the world's most well-managed companies are been victimised by vendor negligence, with costs running into the billions. What attendees will learn: • How to anticipate concerns about third-party risk • Understand how cultural risk plays an important role in third-party risk • Add a business lens to your third-party programme. Learn how you can go from being a risk mitigator to business enabler • Overcome the scrutiny of audits, reviews and investigations with a systematic, pre-emptive approach to third-party risk management • Centralise third-party lifecycle management for all vendor contracts and agreements, due diligence data and risk assessments
SecureData **Battlefield Earth 2018: It used to be security was a network thing** **Charl van der Walt,** Chief Strategy Officer, SecureData	Firewalls, proxies, IDS/IPS, VPNs, network vulnerability scanners. THOSE were the tools of any pureblood security practitioner. Well, those days are gone dear friends. The perimeter is dead and the battle is now on the desktop. Phishing, malicious ads, browser exploits, macros, malware, DDE and malicious mail rules now, well, rule. Since the launch of the Jericho Forum in 2004 we've all know that perimeter is 'dead'. But rapid attacker evolution in the last few months have finally proven this with a force we can no longer afford to ignore. What attendees will learn: • Discover what security leaders like Google are doing in this space • See these attacks in action in real-life environments • Consider that it's time to put aside your network skills and rapidly develop some deep security skills in Exchange, Windows Desktop, Browsers, Outlook and Microsoft Office
Skyhigh Networks/ McAfee **With Cloud, BYOD and remote working – how do you control your data?** **Nigel Hawthorn,** EMEA & Privacy Spokesperson, Skyhigh Networks/ McAfee	Computing is being hit by more changes today than ever before. Mobility, Cloud and BYOD are no longer new and different, but normal and assumed to be the default technologies for new applications and many users. Meanwhile, data loss incidents continue to grow in number and severity and consumers and lawmakers are realising the potential privacy problems of data sharing and big data. With increasing expectations from users, what are the next steps for innovation? What attendees will learn: • Recent trends and how can we get ahead of the data security problems • How to assess what end users want and what they really need • What governance needs, reduce risk and enable innovation even when data isn't just inside the company any more or even travelling via a controlled network
Tessian **What were the causes behind the biggest data breaches in 2017?** **Henry Trevelyan Thomas,** Head of Client Development, Tessian	What attendees will learn: • Rules-based vs Machine intelligence – the big shift in technology • Misaddressed emails were the biggest form of data loss in 2017 – why and how? • How to protect your company against the biggest threats in e-crime by email

Education Seminars

TITUS

Oversharing and the Cloud generation. What will data protection look like in the future?

Don Chadwick, Technical Account Manager, TITUS

When speed and availability are valued over data security, what impact does that have on the viability of your organisation? As a new generation of workers, the Cloud generation, is just beginning to enter the corporate environment, we can learn a lot about what future data protection challenges will look like from the way that this first generation of truly digital natives use and share information.

In parallel, legislation across the world is mandating more responsibilities for data processors and more power to the citizens who can feel they have lost control of their personal information. The financial and reputational impact of a data breach is increasing, so how are organisations to prevent a breach while taking advantage of Cloud technologies and truly digital native workers?

What attendees will learn:

- Preparing for the next generation of data risk, both human and technological
- The challenges of machine learning for data identification
- The future of digital documents in a Cloud-based world
- The impending death and re-birth of cryptology

Trend Micro

Strategies for securing the three classes of IoT

William J. Malik, VP Infrastructure Strategies, Trend Micro

What attendees will learn:

- Plotting the evolution of OT (Operational Technology) and ICS (Industrial Control Systems) into true IoT and IIoT devices
- Understanding the three forms of network-enabled devices that emerge and why they are distinctly different
- Securing these devices requires different approaches to address the architectural limitations of each
- Understanding these differences will allow businesses to set a risk mitigation approach appropriate to each

Wombat Security Technologies

Turning end-user security into a game you can win

Paul Down, Senior Director, EMEA, Wombat Security Technologies

Gamification, as a concept, is nothing new. We'll provide ideas for 'friendly competition' that can ignite interest in your end users and lead to a more successful programme overall.

In this session you'll learn about the cyber topics end users understand the least, based upon research analysing more than 70 million cybersecurity questions asked and answered of end users. We'll offer ideas about the topics you should assess your end users on to create an effective security education programme. Then we'll discuss gamification approaches you can use to get your employees more engaged in your programme and more interested in completing training.

What attendees will learn:

- The cybersecurity topics and best practices that end users struggle to understand
- Techniques that motivate end users to complete training
- Measurement approaches that can help you evaluate your success

ZoneFox

What does the marriage of machine learning and cybersecurity look like in 2018?

Sam Hampton-Smith, Head of Engineering, ZoneFox

Cybersecurity trends come and go, but machine learning looks to be here to stay. Analysts at ABI Research recently reported that there will be an increase in cybersecurity spend on big data, artificial intelligence (AI) and analytics will increase to $96 billion by 2021.
Join us to learn more about getting started with machine learning, where the technology is headed and where it could fit into your security strategy.

What attendees will learn:

- What machine learning can and can't do
- Where machine learning fits into the cybersecurity landscape
- Getting started with ML technology – the challenges and considerations
- What it means for the security team

Cybercrime won't slow down. Take this opportunity to learn from the recent past as you deal with current threats and prepare for whatever's next.