Post event report

Strategic sponsors

CROWDSTRIKE
CYLANCE
DARKTRACE
FLASHPOINT
Hewlett Packard Enterprise
InteliSecure
KASPERSKY
paloalto NETWORKS
PHISHME
QUALYS
SentinelOne
thycotic
wombat security technologies
ZoneFox

Education Seminar Sponsors

BITSIGHT The Standard in SECURITY RATINGS
Centrify
egress
Fidelis Cybersecurity
iboss CYBERSECURITY
Intsights Detect. Analyze. Remediate.
ivanti
mimecast
NTT Security
Secgate
SIXGILL Your Eyes in the Dark Web
THALES
zscaler

Networking Sponsor

REDSCAN

"Thanks for another great year! Really enjoyed all the speakers and the value you get from the breakout sessions is tremendous. Nice to see a lot of focus being given to GDPR and it's going to be interesting to see how it impacts industry in the up and coming months. Looking forward to future AKJ events and thank you again."

VP Cyber Risk, Barclays

"I have been attending for the last 5 years and this incarnation was the most beneficial yet. The Congress gives me the optimal balance of educational input, solution awareness and networking opportunity to keep me up-to-date with developments in the ever advancing cybersecurity landscape."

Group Fraud & Investigations Manager, Lyca Group of Companies

"A very well-organised, very interesting and highly informative event. The talks were top notch and industry-leading and set at a level as to not be 'excluding'. Without hesitation I can say that I am already looking forward to next year's event."

e-Commerce Security Engineer, Office Depot

Inside this report:

Key themes

How do we fix the great cybersecurity disconnect? Time for a radical re-think

Look who's judging you. The challenge of scrutiny

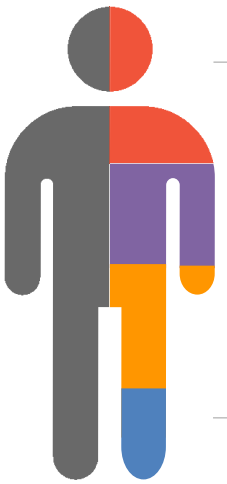
Are you prepared for cybernomics? Cybersecurity is becoming a key driver (and destroyer) of enterprise value. Are you ready for the responsibility?

Law enforcement – the impossible challenge? Can the state protect you against states?

Are you ready for the future? The IoT? AI malware? Automated security?

The scale and sophistication of cybercrime changes everything

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

Sam Alderman-Miller, Darktrace; Amy Baker, VP of Marketing, Wombat Security Technologies; Ken Baylor, President, Vendor Security Alliance; Ivan Blesa, Head of Technology, Secgate; Marinus Boekelo, Digital Expert, Dutch National High Tech Crime Unit; Allan Bower, Regional Director EMEIA, iboss Cybersecurity; Andrew Bushby, UK Director, Fidelis Cybersecurity; Andrew Capon, Consultant, Credit Benchmark; Tim Carolan, Sales Engineer, Thycotic; Ben de la Salle, CISO, Old Mutual Wealth; Jerry Dixon, Chief Information Security Officer, CrowdStrike; Curtis Dukes, Executive Vice President & General Manager, Security Best Practices & Automation Group, Center for Internet Security; Clive Finlay, Director, Office of the CTO, Symantec, on behalf of Intelisecure; Thomas Fitzgerald, Fund Manager, Edentree Investment Management; Josh Galloway, Research Scientist, Cylance; Darron Gibbard CISM, CISSP, Chief Technical Security Officer, EMEA, Qualys; Chris Gibson, Chief Information Security Officer, Banking, Close Brothers; Ian Glennon, Solutions Architect, Qualys; Dr Jamie Graves, CEO, ZoneFox; Nick Green, Director of Information Security at Live Nation Entertainment/Ticketmaster; Ian Greenwood, Regional Sales Manager, Commercial Accounts, Thales e-Security; Richard Hall, Senior Cyber Security Response Analyst, Canada Life; Jim Hansen, COO, PhishMe; Caroline Howard, Territory Manager, Egress Software Technologies; Steven Hutt, Head of Machine Learning, Secgate; Lance James, Chief Scientist, Flashpoint; David Janson, VP Sales UK & Europe, PhishMe; Rajan Kapoor, Head of Data Security, Dropbox, Secretary, Vendor Security Alliance; Alex Karlinsky, Cyber-Intelligence Team Lead, Sixgill; Andy Kennedy, Senior Pre-Sales Systems Engineering Manager, United Kingdom & Ireland, Zscaler; Abdul Khan, Senior Director eCommerce Delivery, Office Depot Europe; Thom Langford, CISO, Publicis; Ryan Lintott, Sales Director, EMEA, InteliSecure; Matt Little, CTO, ZoneFox; Maurits Lucas, Director of Strategic Accounts, Flashpoint; Andrew Martin, Technical Advisor, Secgate; Olivia Mooney, Engagements Manager, UN PRI; Andrey Nikishin, Head of Future Technologies Projects, Kaspersky Lab; Ewen O'Brien, Head of EMEA, BitSight Technologies; Tony Pepper, Chief Executive Officer, Egress Software Technologies; Deepak Rajgor, Systems Engineer WEUR, Palo Alto Networks; Ronald Reukers, Senior Tactical Detective, Dutch National High Tech Crime Unit; Tiago Rosado, Cyber Security Advisor and former Head of Cybersecurity, giffgaff; Andrew Rose, CISO, NATS; Tony Rowan, Director of Security Architecture EMEA, SentinelOne Inc.; Ben Russell, Head of Strategy and Partnerships, NCCU; Barry Scott, CTO, EMEA, Centrify; Garry Sidaway, SVP Security Strategy & Alliances, NTT Security; Andrew Simanski, Chief of Intelligence, Joint Cyber Center; Dan Sloshberg, Product Marketing Director, Mimecast; Spencer Summons, Head of Information Risk and Security, Tullow Oil; Hayley Turner, Darktrace; Zeki Turedi, Lead Security Engineer, CrowdStrike; Jarmo van Lenthe, Digital Crime Investigator, Dutch National High Tech Crime Unit; Sudeep Venkatesh, Global Head of PreSales for Data Security, Hewlett Packard Enterprise; Matthew Walker, VP Security Solutions, Ivanti; Gordon Wallace, Director, Post-Sales EMEA North, Qualys; Professor Tim Watson, Director, WMG Cyber Security Centre, University of Warwick; Paul Watts, CISO, Network Rail; Ido Wulkan, Head of Intelligence, IntSights; Mike Wyeth, Group Security Director, Shopdirect

Agenda | Day 1 | 7th March 2017

07:30 Registration

08:50 Opening remarks

09:00 **Events in cyberspace: Can we keep up?**

Andrew Simanski, Chief of Intelligence, Joint Cyber Center
- Events in cyberspace are moving faster than industry and governments can keep up
- A hat trick of case studies: The OPM hack, the Pentagon Hack, and Black Energy
- Some good news and some bad news: Solutions and what's around the corner

09:20 **Beating cybercrime: Global trends, predictions and the lessons learnt in responding to the most advanced attacks**

Jerry Dixon, Chief Information Security Officer, CrowdStrike
- The current threat landscape – real-life examples of the extraordinary tradecraft routinely employed to steal state secrets, gain access to critical infrastructure or poach valuable intellectual property
- A look to the year ahead – predictions of what you should expect to see and how you should focus your resources to help define strategies to protect your organisation in 2017

09:40 **Ransomware: Is it a special form of crimeware?**

Tony Rowan, Director of Security Architecture EMEA, SentinelOne Inc.
- How has ransomware evolved?
- The trends and likely future directions of ransomware
- How behaviours can be used to isolate ransomware and other forms of malware
- An effective strategy for dealing with malware incidents

10:00 **OODA meets Yoda – the dark side of adaptive security systems**

Professor Tim Watson, Director, WMG Cyber Security Centre, University of Warwick
- Benefits of smart technology and the Observe, Orient, Decide and Act (OODA) loop: Accelerated decision-making, reliability and other business efficiencies
- The dark side. Digital judo, and how your adaptive security system can become an increased target
- Don't underestimate the Force: Solutions, and how to understand the hackers' perspective and use it to your advantage

10:20 **Live demonstration of the Darktrace Threat Visualizer**

Sam Alderman-Miller, Darktrace
- Proving the enterprise value of AI, and how it can protect your business
- Man and machine learning: Can algorithms secure your employees?
- Winning the numbers game: How to effectively employ anomalous behaviour analytics and get actionable results

10:30 **Education Seminar | Session 1** **See pages 7 to 14 for more details**

Centrify	**Stepwise security – a planned path to reducing risk** **Barry Scott,** CTO, EMEA, Centrify
CrowdStrike	**Hacking exposed: Real-world tradecraft of bears, pandas and kittens** **Zeki Turedi,** Lead Security Engineer, CrowdStrike
Fidelis Cybersecurity	**The best of both worlds: A new approach to network and endpoint security** **Andrew Bushby,** UK Director, Fidelis Cybersecurity
InteliSecure	**Understanding your business critical assets** **Ryan Lintott,** Sales Director, EMEA, InteliSecure
IntSights	**Popularisation of cybercrime: Implications and recommendations** **Ido Wulkan,** Head of Intelligence, IntSights
Mimecast	**Cybersecurity is no longer enough, why you need a cyber resilience strategy?** **Dan Sloshberg,** Product Marketing Director, Mimecast
PhishMe	**Artificial intelligence? Isn't it time we all harnessed REAL intelligence to combat cyber attacks?** **David Janson,** VP Sales UK & Europe, PhishMe
Qualys	**Overwhelmed by vulnerabilities? Keep calm and prioritise with Qualys** **Gordon Wallace,** Director, Post-Sales EMEA North, Qualys; and **Ian Glennon,** Solutions Architect, Qualys

11:10 Refreshments and networking break

11:40 **Stepping away from posters and email. The practical solutions to security awareness and engagement**

Thom Langford, CISO, Publicis
- Actionable examples on how to implement cybersecurity awareness
- The importance and impact of a security culture
- What really is the role of the CISO and the security organisation? The answer might surprise you!

12:00 **Collective security – Prairie Dogs vs Humans**

Jim Hansen, COO, PhishMe
- Why the cybersecurity industry is broken
- Reducing susceptibility to human-targeted attacks
- Empower users to become human sensors to recognise and report suspected attacks

12:20 **The Enterprise Immune System: Using machine learning to automate advanced cyber defence**

Hayley Turner, Darktrace
- How machine learning and mathematics can automate advanced threat detection within networks
- Why self-learning technology, known as the 'immune system' approach, detects threats early without using rules or signatures
- How to gain 100% visibility across physical, virtual and cloud environments, including third-party cloud services and SaaS

Agenda | Day 1 | 7th March 2017

12:40 Education Seminar | Session 2 See pages 7 to 14 for more details

BitSight Technologies	**How to manage cyber risk on a daily basis for your company and the affiliates, your suppliers and peers** **Ewen O'Brien,** Head of EMEA, BitSight Technologies
Darktrace	**Darktrace's global threat case studies: A discussion of threats uncovered by the Enterprise Immune System** **Hayley Turner,** Darktrace; and **Sam Alderman-Miller,** Darktrace
Egress Software Technologies	**Securing your organisation and containing the insider threat** **Tony Pepper,** Chief Executive Officer, Egress Software Technologies
Fidelis Cybersecurity	**The best of both worlds: A new approach to network and endpoint security** **Andrew Bushby,** UK Director, Fidelis Cybersecurity
Ivanti	**Ransomware, isn't interested in money anymore… it's your organisation** **Matthew Walker,** VP Security Solutions, Ivanti
Secgate	**Don't take candy from strangers – how behavioural learning is helping in revolutionising cybersecurity** **Ivan Blesa,** Head of Technology, Secgate; **Steven Hutt,** Head of Machine Learning, Secgate; and **Andrew Martin,** Technical Advisor, Secgate
Thycotic	**Non-human privilege accounts – the art of discovering, tokenising and managing machine passwords** **Tim Carolan,** Sales Engineer, Thycotic
Wombat Security Technologies	**Turning end-user security into a game you can win** **Amy Baker,** VP of Marketing, Wombat Security Technologies

13:20 Lunch and networking

14:20 EXECUTIVE PANEL DISCUSSION — The challenge of market scrutiny: The moneymen and the CISO

Olivia Mooney, Engagements Manager, UN PRI; **Thomas Fitzgerald,** Fund Manager, Edentree Investment Management; **Andrew Capon,** Consultant, Credit Benchmark

14:50 Machine learning and the insider threat

Matt Little, CTO, ZoneFox

Join us for the latest ZoneFox thinking for insights around:

- Why machine learning has taken centre stage in 2017 – what it promises and whether it can deliver
- Do you really need machine learning to protect sensitive data?
- SIEM, DLP and the 'old ways' – are they enough?
- What a good machine learning solution needs to be able to do to support your security posture and defend against threats
- The future of machine learning as the threat landscape evolves faster than we can keep up

15:10 Cybercrime: Man vs Machine

Deepak Rajgor, Systems Engineer WEUR, Palo Alto Networks

Media headlines relating to breaches worldwide are testament to both the ever increasing complexity of cybercrime and the failure of organisations to keep pace with criminals by integrating and automating proactive measures. Join us to understand how adversaries plan and execute such crimes and how to successfully disrupt them using an automated and prevention oriented security posture.

- How automation has made attacks cheaper, repeatable and harder to recognise
- The steps attackers use to infiltrate an organisation
- How automation can be used by defenders to stop successful cyber attacks and reduce risk as a preventative security strategy

15:30 Education Seminar | Session 3 See pages 7 to 14 for more details

BitSight Technologies	**How to manage cyber risk on a daily basis for your company and the affiliates, your suppliers and peers** **Ewen O'Brien,** Head of EMEA, BitSight Technologies
iboss Cybersecurity	**Cybersecurity in the distributed world** **Allan Bower,** Regional Director EMEIA, iboss Cybersecurity
Ivanti	**Ransomware, isn't interested in money anymore… it's your organisation** **Matthew Walker,** VP Security Solutions, Ivanti
Sixgill	**Cyber risk assessment through automated threat actor profiling and analysis** **Alex Karlinsky,** Cyber-Intelligence Team Lead, Sixgill
Thales e-Security	**Proactive defence for the digital transformation** **Ian Greenwood,** Regional Sales Manager, Commercial Accounts, Thales e-Security

16:10 Refreshments and networking break

16:30 The evolution of DDoS IoT malware

Lance James, Chief Scientist, Flashpoint

- Technical analysis and comparison of botnets from gafgyt to Mirai
- Common exploitable vulnerabilities in IoT
- Current defensive countermeasures
- Attribution efforts

16:50 EXECUTIVE PANEL DISCUSSION — Coping with innovation: Securing the customer

Nick Green, Director of Information Security at Live Nation Entertainment/Ticketmaster; **Mike Wyeth,** Group Security Director, Shopdirect; **Abdul Khan,** Senior Director eCommerce Delivery, Office Depot Europe; **Tiago Rosado,** Cyber Security Advisor and former Head of Cybersecurity, giffgaff

17:10 Working together to tackle cybercrime

Ben Russell, Head of Strategy and Partnerships, NCCU

- The National Crime Agency's view on the cybercrime threat
- Our operational response: How UK law enforcement targets cybercriminals
- Working in partnership: The need for a joint response

17:30 Drinks and networking | **18:30** End of Day 1

Agenda | Day 2 | 8th March 2017

08:00 Registration

08:50 Opening remarks

09:00 **Surviving the vendor ecosystem: Why the current system is broken and what needs to change**

Ken Baylor, President, Vendor Security Alliance; and **Rajan Kapoor,** Head of Data Security, Dropbox, Secretary, Vendor Security Alliance

- Why the current vendor ecosystem is broken (board level engagement, business risk etc.)
- How secure is your vendor? Why does this affect you? The need for greater scrutiny and benchmarking
- Case study: The VSA's project on benchmarking and analysing vendor security solutions: what's around the corner, and how to deal with it

09:20 **Exploring the mechanics and economics of cybercrime: Recent trends and highlights**

Josh Galloway, Research Scientist, Cylance

- Overview of current attacker community/climate
- Current campaigns and TTP highlights
- Mechanics and methods
- Mitigations and countermeasures

09:40 **Protecting a tsunami of data**

Sudeep Venkatesh, Global Head of PreSales for Data Security, Hewlett Packard Enterprise

- While a deluge of data in recent years can deliver valuable insights and analytics to help organisations innovate, this also presents new security challenges and attack vectors
- Innovations in cryptography such as Format-Preserving Encryption (FPE) are enabling organisations to adopt a 'data-centric' posture to protect this data at rest, in motion and in use
- Gain insights into the technologies and best practices adopted by firms to deploy data protection solutions to protect their most valuable assets

10:00 **15 years perspective: What has changed and what hasn't**

Mike Wyeth, Group Security Director, Shopdirect

- The digitisation of retail and what that means for cybercrime
- Education, education, what we can learn from the past and what this means going forward
- The challenges for industry, governments and law enforcement, international and national. The potential of partnership and pro activity

10:20 **Education Seminar | Session 4** **See pages 7 to 14 for more details**

Cylance	**The devil's bargain: Targeted ransomware and associated costs** **Josh Galloway,** Research Scientist, Cylance
Flashpoint	**What is this 'Deep and Dark Web' you speak of?** **Maurits Lucas,** Director of Strategic Accounts, Flashpoint
Mimecast	**Cybersecurity is no longer enough, why you need a cyber resilience strategy?** **Dan Sloshberg,** Product Marketing Director, Mimecast
NTT Security	**Embedded cybersecurity for business resilience** **Garry Sidaway,** SVP Security Strategy & Alliances, NTT Security
Palo Alto Networks	**Automating the prevention of cybercrime** **Deepak Rajgor,** Systems Engineer WEUR, Palo Alto Networks
SentinelOne	**Ransomware: Is it a special form of crimeware?** **Tony Rowan,** Director of Security Architecture EMEA, SentinelOne Inc.

11:00 Refreshments and networking break

11:30 **Your security at ransom: The threat of ransomware and how public/private collaboration can provide the solution**

Ronald Reukers, Senior Tactical Detective, Dutch National High Tech Crime Unit; and **Marinus Boekelo,** Digital Expert, Dutch National High Tech Crime Unit

- The threat of ransomware and what you need to know
- Case study, investigation of the Coinvault ransomware by the Dutch National High Tech Crime Unit
- Public/private partnership: How working with Kaspersky and leaders from industry resulted in unlocking tens of thousands of Coinvault victims
- Helping governments and companies fight ransomware together: Creation of the NoMoreRansom platform

11:50 **State of the phish 2017**

Amy Baker, VP of Marketing at Wombat Security Technologies

Despite having a solid security awareness and training programme in place, today's cybercriminals manage to evade even the savviest end users through carefully planned email phishing attacks that are only getting more advanced

- Hear direct feedback from infosec professionals on the latest phishing exploits and vulnerabilities in their organisations and how they are protecting themselves
- Learn about the most devastating types of phishing emails used and how to thwart them
- Gain insight into different industries and how they are performing on different types of simulated phishing templates

12:10 **Securing your journey to the cloud**

Clive Finlay, Director, Office of the CTO, Symantec, on behalf of Intelisecure

- The security challenges for businesses when moving data to the cloud
- Current data protection legislation and the impending GDPR: Warnings and takeaways
- Cloud architecture and information-centric security as a critical consideration

Agenda | Day 2 | 8th March 2017

12:30 Education Seminar | Session 5 See pages 7 to 14 for more details

Centrify	**Stepwise security – a planned path to reducing risk** **Barry Scott,** CTO, EMEA, Centrify
Egress Software Technologies	**Securing your organisation and containing the insider threat** **Caroline Howard,** Territory Manager, Egress Software Technologies
IntSights	**Monitoring for cyber threats: What to look for and how** **Ido Wulkan,** Head of Intelligence, IntSights
ZoneFox	**How to get the most out of user behaviour analytics to successfully bolster your security posture and meet tough regulatory compliance requirements** **Dr Jamie Graves,** CEO, ZoneFox
Zscaler	**Zero day defence from day one** **Andy Kennedy,** Senior Pre-Sales Systems Engineering Manager, United Kingdom & Ireland, Zscaler

13:10 Lunch and networking

14:10 Next generation cyber strategy

Spencer Summons, Head of Information Risk and Security, Tullow Oil
- Why achieving digital situation awareness will become the new norm
- Centralising the effort to both protect and create organisation value
- CISO as the next COO/CEO? Why not, after all we will know more about the business than the business

14:30 IoT: The Internet of Things or Internet of Threats?

Andrey Nikishin, Head of Future Technologies Projects, Kaspersky Lab
- The price enterprises pay for a revolutionary age of data, clouds and connected hardware
- The business responsibility of a new safety and privacy dimension: active information security
- The current and forthcoming malware trends heading to IoT and how to prepare for it

14:50 Security as an enabler to digital transformation

Darron Gibbard CISM, CISSP, Chief Technical Security Officer, EMEA, Qualys
- How do organisations gain visibility and insight into their environments?
- How can a move to a SaaS provider provide more visibility and control in your day 2 day strategic operations?
- How have Qualys supported customers to take on the challenge of shadow IT?

15:10 The evolution of passwords

Tim Carolan, Sales Engineer, Thycotic
- 300 billion passwords will be at risk by 2020 – should you be concerned?
- The incredible proliferation of passwords – why they will continue to be necessary?
- Exploring the difference between human and non-human privilege accounts and why this distinction will ultimately lead to enhanced organisational security

15:30 Refreshments and networking break

15:50 EXECUTIVE PANEL DISCUSSION Defending cyber-physical AND digital assets: The latest thinking

Andrew Rose, CISO, NATS
Jarmo van Lenthe, Digital Crime Investigator, Dutch National High Tech Crime Unit
Paul Watts, CISO, Network Rail

16:10 EXECUTIVE PANEL DISCUSSION Risk budgeting, metrics and the challenge of stakeholder engagement

Richard Hall, Senior Cyber Security Response Analyst, Canada Life
Ben de la Salle, CISO, Old Mutual Wealth
Chris Gibson, Chief Information Security Officer, Banking, Close Brothers

16:30 From Groundhog Day to Independence Day: Scripting your cyber defence movie

Curtis Dukes, Executive Vice President & General Manager, Security Best Practices & Automation Group, Center for Internet Security
- Knowing about flaws doesn't get them fixed
- The bad guy doesn't perform magic
- There's a large but limited number of defensive choices
- Cyber defence => Information management
- Cybersecurity is more like 'Groundhog Day' than 'Independence Day'

16:50 Closing remarks **17:00** End of Day 2

Education Seminars	
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)** Presenter: Ewen O'Brien, Head of EMEA, BitSight Technologies	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 the company and the affiliates, the suppliers and peers can be managed based on qualified events and ratings
Centrify **Stepwise security – a planned path to reducing risk** Presenter: Barry Scott, CTO, EMEA, Centrify	Attackers are making major headway into our businesses with simple tactics that exploit our weakest points. What attendees will learn: • Proven practices for prioritising a risk mitigation strategy • Easy gaps that most often lead to data breach • Steps to gain sophisticated and comprehensive control
CrowdStrike **Hacking exposed: Real-world tradecraft of bears, pandas and kittens** Presenter: Zeki Turedi, Lead Security Engineer, CrowdStrike	This session explores the evolution of threats – from discrete criminal events to an offensive weapon. We'll lift the lid on the latest attack techniques, adopted by nation state actors, which invariably find their way into the mainstream criminal world and are therefore an indicator of what to prepare for. Zeki will reference who the most active and advanced adversaries are, what attack vectors they typically employ, and how we can apply this intelligence to prevent, protect and respond. Using simulated attack scenarios and personal examples of the speaker's experience, attendees will learn how to spot indicators of compromise and attack, and how to safeguard their organisation accordingly. What attendees will learn: • How nation-state threats are crafted and how their Tactics, Techniques and Procedures (TTPs) help identify them from more routine advanced attacks • Who are the most notable adversaries in 2017 and the key European security themes based on the latest intelligence compiled across CrowdStrike's global intelligence gathering operation • What are the indicators of attack and how you can apply them to defeat the adversary?
Cylance **The devil's bargain: Targeted ransomware and associated costs** Presenter: Josh Galloway, Research Scientist, Cylance	Ransomware is the most direct way to monetise cybercrime, and there is a trend towards ransomware being more targeted to maximise the odds of a payout. Targeting hospitals and medical devices, for example, because when lives are at stake, there isn't necessarily time to restore from backup. This talk will cover some other likely targets for more coordinated ransomware campaigns in 2017, and what organisations can do to prevent being put in these lose-lose predicaments in the first place. What attendees will learn: • Examples of the trend towards more targeted ransomware • Where we should expect to see more coordinated ransomware attacks in the future • Costs of mitigation in these contexts • What organisations can do to minimise risk • Why traditional signature-based AV fails

Education Seminars

Darktrace

Darktrace's global threat case studies: A discussion of threats uncovered by the Enterprise Immune System

Presenters: Hayley Turner, Darktrace; and Sam Alderman-Miller, Darktrace

With over 2,000 deployments worldwide and offices in over 20 countries, Darktrace's Enterprise Immune System has detected more than 27,000 'serious' early-stage threats that went unnoticed by legacy security tools. Darktrace has unique experience of in-progress attacks and novel threat patterns that have been mitigated before escalating into full-blown crises.

This session will illuminate the kind of threats that Darktrace is capable of uncovering, using Darktrace's self-learning technology. Each case study presents a unique circumstance, in which abnormal behaviours have been identified by Darktrace, while the threat situation was still 'live' and developing. No rules and signatures, or prior knowledge of the network or threat landscape, are used to detect the anomaly. Instead, the Enterprise Immune System uses advanced mathematics and machine learning to quickly understand what 'normal' behaviour looks like in the network, highlighting emerging threats in real time – and responding to them automatically.

What attendees will learn:

- Real-world examples of in-progress threats uncovered by Darktrace, including the compromise of a video-conferencing camera and fast-moving targeted ransomware, and how they were mitigated
- How the Enterprise Immune System detects threats that go unnoticed by legacy security tools, such as long-term cyber missions and insider threats
- Why Darktrace's technology, powered by machine learning and mathematics, has been globally deployed across all industry verticals in physical, virtual and cloud environments

Egress Software Technologies

Securing your organisation and containing the insider threat

Presenter: Tony Pepper, Chief Executive Officer, Egress Software Technologies

Despite increasing investment in the cybersecurity market, we continue to see a rise in data breaches and their related costs, specifically those relating to the insider threat (both accidental loss and malicious insider).

Yet, even though these types of incidents now contribute approximately 50% of all data breaches, CIO focus remains on defeating the external threat (hacking and network-related attacks).

This presentation will examine the benefits of a new approach to data security – one that recognises data security threats can't be tackled in silo but instead must be both holistic and strategic, and shining a light on how to overcome data breaches through accidental loss and malicious insider. Ultimately, we will discuss the steps required to protect and secure data throughout its lifecycle in order to contain the insider threat.

What attendees will learn:

- The benefits of a new holistic approach to data security in order to overcome the rising trend in data breaches
- How to identify, understand and overcome the insider threat within your organisation
- Ways to implement information security solutions that address the 'lifecycle' of data protection, from creation to secure data release
- How this approach can directly improve compliance with industry and data protection legislation

Fidelis Cybersecurity

The best of both worlds: A new approach to network and endpoint security

Presenter: Andrew Bushby, UK Director, Fidelis Cybersecurity

Today's organisations are increasingly facing the reality that they are fighting against cybercriminals with yesterday's solutions. APTs are evolving and since traditional Intrusion Prevention Solutions (IPS) were designed to identify attacks targeting known vulnerabilities, there are some serious new threats and threat actors slipping through the net.

Join Andrew Bushby to find out about Fidelis' next-generation IPS that unifies both Fidelis network and endpoint products to detect and stop modern intrusions at every stage of the attack lifecycle.

What attendees will learn:

- Detect intrusions traditional IPS can't see
- Reduce time to respond and resolve threats by 15x
- Optimise your security stack

This session is based on a demo performed in front of the audience

Education Seminars	
Flashpoint **What is this 'Deep and Dark Web' you speak of?** **Presenter:** Maurits Lucas, Director of Strategic Accounts, Flashpoint	The Deep and Dark Web: What is it and why should you care? In this session, Maurits Lucas, Director of Strategic Accounts at Flashpoint, will dispel some persistent myths about the Deep and Dark Web, outline some of the challenges involved in effectively tracking and monitoring threats on the DDW, and use examples to demonstrate how what is going on in the dark nooks and crannies of the internet is relevant to organisations across the globe, and can be leveraged to mitigate company-wide risk. This session will conclude with an update on the current trends and threats emanating from the Deep and Dark Web. What attendees will learn: • What is the Deep and Dark Web? Distinguishing truths from common misperceptions • The challenges for organisations tracking threats on the Deep and Dark Web • What is required to effectively glean actionable intelligence • How the Deep and Dark Web affects the visible web • Update on current trends and imminent threats in the Deep and Dark Web
iboss Cybersecurity **Cybersecurity in the distributed world** **Presenter:** Allan Bower, Regional Director EMEIA, iboss Cybersecurity	Join Allan for an overview of the unique and innovative technologies that power the iboss cybersecurity platform. Learn how iboss is uniquely positioned to help distributed organisations secure all devices, anywhere. What attendees will learn: • The pedigree and strength behind the iboss platform • The innovative iboss node-based architecture • The platform for unique partnerships
InteliSecure **Understanding your business critical assets** **Presenter:** Ryan Lintott, Sales Director, EMEA, InteliSecure	All businesses have informational assets that are critical to their business operations, but the following are not always understood: what that content is, where it resides, where it should be, what community currently has access to, who should have access. Ryan Lintott will explain how you can go about this and discuss the Critical Asset Protection methodology which you can adopt. What attendees will learn: • Protect your sensitive content: through which channels is sensitive data being transmitted and what channels should be used? • With GDPR on the horizon and the increasing about of breaches, how can you understand and protect your content? • Protect your critical assets: protect your business. How to manage sensitive content that is critical to business operations
IntSights **Popularisation of cybercrime: Implications and recommendations** **Presenter:** Ido Wulkan, Head of Intelligence, IntSights	The past couple of years have seen a steep rise in online services that offer individuals 'easy access' to the world of cybercrime. Such services include cloud-like malware and ransomware services, Phishing as a Service websites, and scam-shops that make the life of an inspiring hacker much easier than before. At the same time, online black markets has evolved to detect the potential in human-reliant cyber attacks, such as insider information trade, insider privilege exploitation and cyber extortion. Such methods in turn lowered to a record minimum the necessary bar for an individual to partake in cybercrime. The above processes might result in a chaotic threat-ecosystem which entails all organisations, including small-to-medium ones, to have a clear and concrete vision for cybersecurity based on intelligence and decision making. What attendees will learn: • A new way of looking at the cybercrime ecosystem, in an age of threat proliferation and popularisation • Why monitoring of the cybercrime ecosystem is crucial more than ever • How to prepare for and mitigate 'lone-wolf'/low-level cyber threats by combining managerial vision with professional expertise

Education Seminars	
IntSights **Monitoring for cyber threats: What to look for and how** Presenter: Ido Wulkan, Head of Intelligence, IntSights	With the abundance and variety of online information, so does grow the 'white noise' that accompanies it. Extracting the best intelligence out of the deep and dark web requires information to be actionable and concrete. The seminar would explain how a clear categorisation and taxonomy of the threat landscape, along with a persistent presence in online sources and an organised work-plan – could serve a firm basis for a comprehensive intelligence array. What attendees will learn: • A terminological set that would enable them to re-interpret cyber-threat monitoring • An index of expected cyber threats per source-type • A long-term approach for gaining and maintaining access to the deep and dark corners of the web
Ivanti **Ransomware, isn't interested in money anymore… it's your organisation** Presenter: Matthew Walker, VP Security Solutions, Ivanti	Join Matthew Walker, VP of Security Solutions at Ivanti (Formerly Heat Software, LANDESK, AppSense, Shavlik, Wavelink), as he explains how ransomware and the motives behind them are evolving into something more serious than just a demand for cash. The exponential rate of data growth is causing an increase in the attack surface area for cybercrime to capitalise on, leaving not only enterprises but governments, utilities, services providers at risk – which can ultimately bring a country to a standstill. What attendees will learn: • How you can prevent up to 85% of Windows intrusions threats by implementing 4 key disciplines • Why security doesn't have to compromise user experience • How you should prepare your users to be cyber-safe
Mimecast **Cybersecurity is no longer enough, why you need a cyber resilience strategy?** Presenter: Dan Sloshberg, Product Marketing Director, Mimecast	What attendees will learn: • The growing sophistication and scale of cyber attacks • Why traditional defences are no longer sufficient • Key building blocks of a resilience strategy
NTT Security **Embedded cybersecurity for business resilience** Presenter: Garry Sidaway, SVP Security Strategy & Alliances, NTT Security	In today's connected world, cyber maturity, agility and business resilience are inextricably linked. For every organisation wishing to innovate, adapt and grow – understanding and managing cyber risk to the physical and digital infrastructure is an essential competency. Whatever your commercial or technology aspirations, you need to plan, deliver and maintain the necessary cybersecurity for business resilience. What attendees will learn: • Understand the practical implementation of cyber resilience • Increase cyber capability with intelligence in context • A business-resilient approach

Education Seminars	
Palo Alto Networks **Automating the prevention of cybercrime** **Presenter:** Deepak Rajgor, Systems Engineer WEUR, Palo Alto Networks	Contributors to the massive growth of the cybercrime landscape include the convenience, speed and ever reducing costs afforded to attackers through automating their activities. Additionally, advances in the sophistication of cyber attacks over the past decade closely correlate with an increased risk for organisations that maintain manual processes for identification and prevention of these attacks. Join us to learn how an automated security infrastructure can prevent each step of an attack enabling defenders to regain the advantage and reduce that increasing risk. What attendees will learn: • How not all threat intelligence clouds are created equal • How intelligence gathered about the threat landscape is used to mitigate the various stages of an attack • Why an integrated platform can provide the automation required to meet security's rapidly evolving challenges
PhishMe **Artificial intelligence? Isn't it time we all harnessed REAL intelligence to combat cyber attacks?** **Presenter:** David Janson, VP Sales UK & Europe, PhishMe	Phishing and spear phishing remain the No. 1 attack vector threatening organisations worldwide, continuing to challenge IT security teams as threat actors evolve their tactics to gain access to corporate networks, assets and consumer data. Now, more than ever, organisations must be able to understand and identify the successful types of email attacks, themes, and elements used to successfully phish employees so that we can determine how best to prepare and condition them to identify and report suspicious emails to internal IT security teams. Perimeter defences, however robust, cannot and will not stop all phishing emails. Sooner or later, someone will click, so how can the time to detection of an initial infection be brought down, to lengthen the opportunity to prevent a larger attack. What attendees will learn: • Learn the latest methods being used in phishing attacks • Discover which phishing themes and emotional motivators users find the most difficult to recognise and report • Learn how behavioural conditioning can be utilised to form a human phishing defence
Qualys **Overwhelmed by vulnerabilities? Keep calm and prioritise with Qualys** **Presenters:** Gordon Wallace, Director, Post-Sales EMEA North, Qualys; and Ian Glennon, Solutions Architect, Qualys	Finding vulnerabilities, compliance exceptions or web application risks in any organisation is easy; making them go away is a much more difficult task. While the theoretical 'Fix-It' button may be stuck in the up position, we will share real experiences of how to lubricate the workflow of risk mitigation with the people, process and technology conundrum. What attendees will learn: • Gain full visibility and control of all IT assets to effectively ensure security and compliance • Automatically prioritise the vulnerabilities that pose the greatest risk to your organisation • Measure your progress and remediation efforts with real-time trend analysis

Education Seminars

Secgate

Don't take candy from strangers – how behavioural learning is helping in revolutionising cybersecurity

Presenters: Ivan Blesa, Head of Technology, Secgate; Steven Hutt, Head of Machine Learning, Secgate; and Andrew Martin, Technical Advisor, Secgate

"Don't take candy from strangers" is one of the first things parents tell kids when they face the threats of the outside world. It is a sensible approach – children know their parents and the adults that they trust – everyone else poses a risk that they should avoid. But how can we translate this approach into the realm of cyber protection?

Organisations are commonly trying to protect themselves by looking for known patterns of malicious activity. This ranges from antivirus to full teams of SOC analysts using the latest detection technologies. But this approach is not detecting all threats and hence we have massive data breaches. Threats are often unique to each organisation, so detection systems based on knowing what malicious activity looks like tends to fail.

Advances in data extraction, data analysis and machine learning techniques allows us to propose an innovative way to cyber protection. This approach offers protection based on real data taken from within an organisation, not on external information that doesn't apply to one. This session examines this key concept, highlighting previous blockers within the field, and how these are being overcome. We will look at the complexity of applying this simple concept into real use cases and comparing them with how the security market is evolving.

Our talk will explore the different ways in applying intelligent analysis to the right data sets to perform behavioural learning in its full capacity, and why settling for a standard solution is not enough when you can understand and obtain an advanced approach.

What attendees will learn:

- The generic stranger – why traditional approaches are failing to identify malicious activity
- Why intrusions go undetected
- The difference behavioural learning techniques can have in the realm of cybersecurity
- What data samples behavioural learning techniques need – and how these can be obtained
- How theoretical solutions can be brought to reality

SentinelOne

Ransomware: Is it a special form of crimeware?

Presenter: Tony Rowan, Director of Security Architecture EMEA, SentinelOne Inc.

In Tony Rowan's session you will explore the evolution of ransomware and gain insights into where this contagion is moving. The session will explore the commonalities with other forms of malware but will also expose the key differences in the approaches used. The analysis will demonstrate how malicious behaviours can be used to determine ransomware and other forms of malware, showing an effective strategy for incident handling.

What attendees will learn:

- How has ransomware evolved
- The trends and likely future directions of ransomware
- How behaviours can be used to isolate ransomware and other forms of malware
- An effective strategy for dealing with malware incidents

Sixgill

Cyber risk assessment through automated threat actor profiling and analysis

Presenter: Alex Karlinsky, Cyber-Intelligence Team Lead, Sixgill

What attendees will learn:

- Threat actor analysis using automated dark web intelligence tools
- Automated intelligence gathering as a force multiplier
- Dissecting and analysing threat actor activity
- Case study

Education Seminars	
Thales e-Security **Proactive defence for the digital transformation** Presenter: Ian Greenwood, Regional Sales Manager, Commercial Accounts, Thales e-Security	As UK organisations set out on their path to digital transformation, there can be no denying that more and more services will be brought online and moved into the cloud – from tax returns to healthcare records – making a faster, more agile and open service for consumers and enterprises. However, such transformation is happening within an increasingly precarious environment – one in which data breaches are at an all-time high and incidents of identity theft have risen by 57% in a single year. Data is the prize for these hackers and, as more services are moved into the cloud, the concern for many UK citizens will be around their valuable, personal data falling into the hands of those with malicious intent. With the rise of cloud and the Internet of Things, it's evident the threat of attack has moved from the perimeter to within an organisation's walls, and consequently measures need to be put in place to take control of data – regardless of where it resides. Join Ian Greenwood, Regional Sales Manager of Thales e-Security for an interactive and informative discussion. What will attendees learn: • What are key considerations when engaging on a digital transformation strategy • Why organisations should take a proactive data defence strategy when it comes to digital transformation • The benefits of maximising the level of control over data irrespective of where it created, stored or shared
Thycotic **Non-human privilege accounts – the art of discovering, tokenising and managing machine passwords** Presenter: Tim Carolan, Sales Engineer, Thycotic	Tim Carolan looks at the best ways to identify and deal with privileged credentials that are not attached to a human user, highlighting common pitfalls of being without a software solution capable of bringing these passwords under management. What attendees will learn: • Common types of machine and non-human passwords and why enterprises should be concerned about them • Techniques for machine account discovery and management • How to deploy and manage tokenisation on all privileged passwords
Wombat Security Technologies **Turning end-user security into a game you can win** Presenter: Amy Baker, VP of Marketing, Wombat Security Technologies	Gamification, as a concept, is nothing new. We'll provide ideas for 'friendly competition' which can ignite interest in your end users and lead to a more successful program overall. In this session you'll learn about the cyber topics end users understand the least, based upon research analysing 20 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 program. Then we'll discuss gamification approaches you can use to get employees to complete training. What attendees will learn: • The cybersecurity best practice that end users struggle to understand • Techniques that motivate end users to complete training • Measurement approaches that can help you evaluate your success

Education Seminars	
ZoneFox **How to get the most out of user behaviour analytics to successfully bolster your security posture and meet tough regulatory compliance requirements** Presenter: Dr Jamie Graves, CEO, ZoneFox	If you don't plan ahead before implementing a UEBA security solution, you're going to find it an uphill struggle, unlikely to see the business benefits you were expecting. Join us for this latest ZoneFox seminar to gain valuable insights around what you should be thinking about when considering a UEBA solution, how best to prepare before your business implements this type of security platform, and where you can expect to reap the rewards – from successful threat mitigation, to intelligent support around meeting regulatory compliance. What attendees will learn: • Learn how UEBA solutions are currently used – from predictive control to risk assessment to helping shape a robust security posture • Gain insights around how to get the most out of UEBA before implementation (what you need to focus on – eg, a clear understanding of the business objectives, the threat environment, existing controls, and UEBA's capabilities etc) • Discover the ways in which business can be supported by UEBA – from intelligent threat management, to support in meeting GDPR compliance and ensuring success/preparedness in meeting the much-talked-about 72-hour breach disclosure requirements • How to work with the information and insights that your UEBA solution provides
Zscaler **Zero day defence from day one** Presenter: Andy Kennedy, Senior Pre-Sales Systems Engineering Manager, United Kingdom & Ireland, Zscaler	With over 30 billion web transactions a day and over 120 million new strains of malware being detected in the past 12 months, total zero-day protection is a must for any organisation. During this session we will review some of the insights and lessons learned from 2016 and will discuss a security methodology based on Zscaler's integrated platform to deliver a complete security stack in the cloud, providing day zero protection from day one. What attendees will learn: • Recommendations to protect your organisation in today's social and mobile world • Discover the impact of one wrong download • How to increase business agility, eliminate unnecessary costs and still provide a fast user experience • How to secure your organisation from day one with a complete security platform