Post event report

The 10th e-Crime & Cybersecurity Mid-Year Summit

18th October 2018 | London, UK

Strategic Sponsors

BOMGAR

FIREMON

IBM Resilient

mimecast

NTT Security

SECURE DATA
TRUSTED CYBERSECURITY EXPERTS

ZoneFox

Education Seminar Sponsors

activereach

DEMISTO

egress

EQUINITI
CYBER SECURITY

esentire

GROUND LABS

ORACLE
Dyn

OSIRIUM

PLURALSIGHT

Networking Sponsors

GARRISON

IDECSI
Enterprise Security

Jazz Networks

REDSCAN

CS CYBER SCORE
BY XQ CYBER

Branding Sponsor

AGARI

> “This was my third visit and once again the speakers were excellent and they condensed lots of relevant and interesting information within their presentations. The elective breakout seminars give a more in-depth look at topics, and the network breaks allowed me to speak to vendors about their products and services.”
>
> **Head of Risk – IT & Cybersecurity, Paragon Bank**

> “e-Crime & Cybersecurity Mid-Year Summit is a great place to engage with peers on current problems and security trends in a relaxed and informative atmosphere.”
>
> **European Business & Information Security Specialist, Canon Europe**

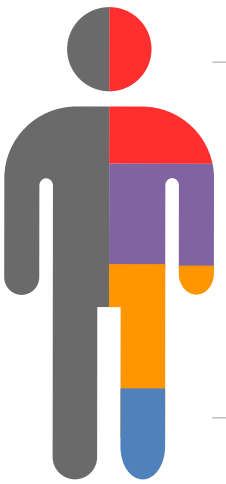
> “This is a great event which has many informative presentations from vendors and business sectors. I also use this time to meet new and old colleagues to exchange knowledge and points of view.”
>
> **EMEA Operational Security Manager & Business Line Security Officer, SGCIB**

Inside this report:

Key themes

- Keeping up with the regulators
- Cybersecurity: a core risk management discipline
- Ensuring enterprise scalability
- Cybersecurity for the SME
- Taking third-party security seriously
- Cyber-physical security: a holistic approach
- Intelligence-based cybersecurity
- Prepare for transparency now

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

Azeem Aleem, VP Consulting & Head of UK Business, NTT Security

Tommy Barlow, Director EMEA, Pluralsight

Steve Benton, Deputy CSO, BT

John Cassidy, Global Sales Leader, Ground Labs

Chris Clarkson, Senior Solutions Engineers, Bomgar

Ryan Collier, Key Account Executive, Egress Software Technologies

Phil Cordey, Group Head of IT Security, Inchcape

David Doherty, Global IM Cyber GRC and Technical Assurance Specialist, Anglo-American

Etienne Greeff, CTO, SecureData

Andy Harris, Chief Technology Officer, Osirium

Paul Holland, Information Security Consultant, Hiscox

Simon Jenner, CISO, Booking.com

Kostas Lotsis, Technical Sales Engineer, FireMon

Craig McEwen, Global Head of Cyber Operations, Anglo-American

Richard Merrygold, Director of Group Data Protection, HomeServe

Joe Nelson, Principal Solutions Architect, eSentire

David Porter, Head of Innovation, Security and Privacy Division, Bank of England

David Staunton, Product Marketing Manager, Mimecast

James Stevenson, Sales Director - UK, Nordics and Benelux, Demisto

Jonny Tennyson, Head of Customer Success, ZoneFox

Jon Townsend, CIO, National Trust

Chris Underhill, Chief Technology Officer, Equiniti

Ivan Virgili, Partners & Alliances Account Director, EMEA & APAC, Oracle + Dyn

Paul Watts, CISO, Domino's

Simon Wood, VP Cyber Investigations Manager, Barclays

Simon Wright, Group Data Protection Officer, Photobox Group

Andy Yeates, Solutions Architect, IBM Resilient

Agenda

08:00 Registration and breakfast networking

08:50 Chairman's welcome

09:00 **Different sector, same old sh... the cross-sector basics we're still failing to get right**

Paul Watts, CISO, Domino's

- Looking at cybersecurity from the retail, then CNI and then QSR sector. Contrasts and comparisons
- Why we are still failing to get some of the basics right when it comes to good security hygiene?
- Building cyber-maturity. Navigating the cyber-spam and finding new solutions to continuing threats

09:20 **Intelligence-driven security: where the rubber hits the road**

Azeem Aleem, VP Consulting & Head of UK Business, NTT Security

- Reducing risk and protecting sensitive information assets is paramount to organisations' financial well-being
- A robust tactical operations strategy is required to proactively detect, deny and remediate the advanced persistent threats (APTs) impacting both public and private enterprises
- Hear how to embed intelligence-driven security within your organisation's environment, using a tactical approach and predictive analytics

09:40 **Seconds out! When algorithms don't play nice with our applications and lives**

Etienne Greeff, CTO, SecureData

- Debunking facts around artificial intelligence in respect to cybersecurity
- High-level view on AI & machine learning and how these can be used in both offensive and defensive applications
- Practical examples of AI-based defences
- Recommendations for how this technology can be used within your networks and applications

10:00 **GDPR & global privacy frameworks**

Richard Merrygold, Director of Group Data Protection, HomeServe

- Maintaining an established governance structure and working with regulators and requirements, both for your business and your customers
- Verifying and monitoring of information security protocols
- Adhering to a company-wide data breach response programme

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

Egress Software Technologies	Equiniti	Ground Labs
Securing email – so much more than just encryption **Ryan Collier,** Key Account Executive, Egress Software Technologies	**Cyber-risk in the supply chain** **Chris Underhill,** Chief Technology Officer, Equiniti	**Standards don't bother me – all I want is your data!** **John Cassidy,** Global Sales Leader, Ground Labs

11:00 Networking and refreshments break

11:30 **You are a target – find it and fix it before someone else breaks it**

David Doherty, Global IM Cyber GRC and Technical Assurance Specialist, and **Craig McEwen,** Global Head of Cyber Operations, Anglo-American

- Internal and external pressures on your organisation requiring you to manage data effectively
- Why Tick Box compliance is not good enough
- Technical assurance – proving the controls work as expected

11:50 **PAM: the critical missing piece in your security strategy**

Chris Clarkson, Senior Solutions Engineers, Bomgar

What attendees will learn:

- Understand the critical importance of securing 'privilege' in your organisation
- Leave with the tools to understand the scope of your organisation's Privileged Access Management (PAM) project
- Gain top tips to prepare your PAM project business case for successful sign off

12:10 **Cybersecurity: the modern business has no perimeter**

Jonny Tennyson, Head of Customer Success, ZoneFox

- Insider attacks are on the rise – a cyber-strategy focused on protecting the perimeter is futile
- Employees are now the perimeter and they're always on the move; remote working opens organisations up to increased risks surrounding their data
- What does the insider threat look like?

12:30 **The two sides of cyber-resilience; people and technology**

David Staunton, Product Marketing Manager, Mimecast

- The critical role that email plays in your cyber-resilience strategy
- The rise, and increasingly vulnerability, of the human firewall and how to protect your users and organisations
- The importance of being able to deal with a compromise when, not if, it will happen

Agenda

12:50 Education Seminars | Session 2

Oracle + Dyn in partnership with activereach	Demisto	Osirium
In light of the British Airways data breach & other high-profile hacks, how should businesses adapt their approach to web application security? **Ivan Virgili,** Partners & Alliances Account Director, EMEA & APAC, Oracle + Dyn	**The blessing and the curse – the unintended outcome of SIEM driving the SOAR market** **James Stevenson,** Sales Director - UK, Nordics and Benelux, Demisto	**How passwords get stolen, how attackers move laterally across networks, how to separate people from the passwords, how to add multifactor authentication to systems that don't natively support it** **Andy Harris,** Chief Technology Officer, Osirium

13:30 Lunch and networking

14:30 Riding the AI wave: tips for staying dry

David Porter, Head of Innovation, Security and Privacy Division, Bank of England

- Expectations are high as the promise of an exciting new generation of artificial intelligence appliances resonates with businesses and consumers
- But we've been here before, only for excitement to give way to disappointment as the hype fails to deliver. We should proceed with caution
- After a couple of false starts, and despite varying definitions, artificial intelligence is enjoying a new lease of life courtesy of big computing, big data and big social
- The latest FinTech initiatives are showing that the lessons learned by the original artificial intelligence pioneers are still relevant today, if not more so
- And as artificial intelligence pushes the boundaries of automation, new models of how we think and work compel us to better understand the potential for artificial error

14:50 The journey of incident response

Andy Yeates, Solutions Architect, IBM Resilient

- Organisations today need to be agile, and dynamic in responding to the most advanced cyber-threats. How is the landscape changing and what is the impact on security?
- What is automation's place in improving SOC efficiencies and how does it measure up to human intelligence in effective incident response?
- The journey to intelligent orchestration and how leveraging it in an uncertain world can empower your organisation

15:10 The time for intent-based security is here...

Kostas Lotsis, Technical Sales Engineer, FireMon

In this session you will learn about:

- Adopting new networking technologies and development processes
- Leveraging automation to turn security intent into security enforcement
- Not having to write another firewall rule
- Strategies for defining security intent in your environment
- Four capabilities necessary to put IBNS into practice

15:30 Education Seminars | Session 3

eSentire	Pluralsight
Cyber-attack trends from the Threatscape **Joe Nelson,** Principal Solutions Architect, eSentire	**The pace of change will never be this slow again – are you on the right side of disruption?** **Tommy Barlow,** Director EMEA, Pluralsight

16:10 Networking and refreshments break

16:30 EXECUTIVE PANEL DISCUSSION — Third parties and toothless regulators: the scary reality of today's post GDPR landscape

Chaired by: Simon Jenner, CISO, Booking.com

Simon Wood, VP Cyber Investigations Manager, Barclays
Jon Townsend, CIO, National Trust
Simon Wright, Group Data Protection Officer, Photobox Group
Paul Holland, Information Security Consultant, Hiscox

16:50 The genie's out of the bottle: the inconvenient truth about cyber-assurance

Steve Benton, Deputy CSO, BT

- What are the cyber-metrics out there telling you? And can you trust them?
- The role of cyber-assurance providers. Don't let metrics be your sole point of reference
- Be careful what you wish for. In the marketplace, cyber-metrics will become increasingly influential. And affect your ability to win business
- Does this, or should this, change your approach to cybersecurity?

17:10 Inconvenient truths: challenges of IT and information security

Phil Cordey, Group Head of IT Security, Inchcape

- How do you handle ever-changing risk?
- Is your security infrastructure 'fit for purpose'?
- Addressing the cyber-risk. Questions and solutions

17:30 Drinks reception and networking

18:30 Conference close

Education Seminars

Demisto

The blessing and the curse – the unintended outcome of SIEM driving the SOAR market

James Stevenson,
Sales Director – UK, Nordics and Benelux,
Demisto

For SOC managers, the SIEM was both a blessing and a curse: it was a way to consolidate and correlate security alerts into a single console, however, the proliferation of new security tools and constantly evolving threats has resulted in SOCs drowning in a flood of security alerts.

Many SOCs are experiencing alert fatigue due to the unsustainable alert levels, and analysts are consequently becoming desensitised. This is leading to longer response times, missed critical events and stress/anxiety. The high turnover rate of security analysts is further compounded by the security industry's persistent talent gap. This has forced some organisations to rethink how they run their SOCs and driving an emerging market Gartner calls SOAR. A SOAR centric approach is designed to help security teams focus on high-value activities by automating repetitive, costly and time consuming tasks. This increases security analyst productivity with fewer resources, while ensuring a consistent and repeatable incident handling process every-time to reduce Mean Time to Resolution (MTTR) and business risk.

The session will go through a brief overview of SOAR, common use cases, a demonstration, and underscore how SOAR platforms help with:

- Coordinating actions across the entire security stack
- Automating repeatable actions with human review and oversight
- Reduce Mean Time to Resolution (MTTR), shaving down response times from hours to seconds

Egress Software Technologies

Securing email – so much more than just encryption

Ryan Collier,
Key Account Executive,
Egress Software Technologies

Email is far from dead. It is estimated that over 281 billion emails are sent globally every day, cementing it as one of the primary mechanisms for business communication. However, when relied upon by staff to share personal data, email also becomes a major cause of data breaches.

Join Egress' Ryan Collier as he examines the ways email security technology can adapt to tackle security threats in a time when organisations are under more legislative pressure than ever before, including the evolution of encryption, preventing user error and risk-based authentication.

- The true risk employees pose by sharing sensitive personal and corporate data via email
- The ways email protection can go beyond encryption to provide the robust security required by today's threat landscape and to comply with increasingly more stringent regulations
- How AI and machine learning can predict users' mistakes and prevent accidental data breaches
- The ways technology can identify malicious email activity by employees to alert administrators to data breaches
- How risk-based authentication can encourage user adoption and improve data protection

Equiniti

Cyber-risk in the supply chain

Chris Underhill,
Chief Technology Officer,
Equiniti

If your supply chain extends beyond your company walls – and beyond your control – it's vulnerable and exposed. Supply chains are a popular target for cybercriminals and are commonly seen as a weak link for providing access to a network of organisations and highly sought-after data.

In this talk we will cover:

- The DNA of a Supply Chain attack, and what we can learn from past compromises
- How to conduct proactive Supply Chain monitoring for signs of compromise
- How can you use Threat Intelligence to identify Supply Chain threats before they become attacks

Education Seminars

eSentire

Cyber-attack trends from the Threatscape

Joe Nelson,
Principal Solutions Architect, eSentire

Defending against evolving threats has never been more important for midsized organisations working to guard against financial and reputational risk.

eSentire's Quarterly Threat Report, produced by the Threat Intelligence Team, provides an overview of the threats detected by the eSentire Security Operations Center (SOC) in 2018. The report analyses threat types, volume, and preferred attack methods based on data gathered from 1500+ proprietary network and host-based detection sensors.

What will you learn:

- What are the latest trends in the cybercriminal underworld?
- Which attacks are you likely to be preventing as we move into 2019?
- Who's looking for vulnerability on your network?

These questions and more, answered by eSentire's Principal Solutions Architect, Joe Nelson.

Ground Labs

Standards don't bother me – all I want is your data!

John Cassidy,
Global Sales Leader, Ground Labs

How a business-as-usual approach to data security and performing sensitive data discovery can aid in achieving PCI and GDPR compliance:

- Insights into how cybercriminals do not comply with global security standards, data theft is their only concern
- Understanding the totality of your data helps in risk assessment for cybercrime
- Data sprawl is one of the key challenges across corporate infrastructure as it presents a huge vulnerability to cybersecurity professionals

Oracle + Dyn in partnership with activereach

In light of the British Airways data breach & other high-profile hacks, how should businesses adapt their approach to web application security?

Ivan Virgili,
Partners & Alliances Account Director, EMEA & APAC, Oracle + Dyn

Web application attacks are the primary cause of data breaches today. In the past year, we have seen Dixons Carphone, Ticketmaster, Butlin's, Equifax & British Airways exposed. The British Airways hack is impressively bad; for more than two weeks this summer, hackers took the personal and financial details of 380,000 customers who made, or changed, bookings on ba.com or its app during that time.

Gartner is telling us that the WAF (web application firewall) market is full of disappointment: security systems designed to secure websites from 2005. Post-breach statistics and analysis from Verizon tell us that data breaches from websites have been growing exponentially since 2010. Veracode tells us that the majority of modern web applications – two thirds of them – leak data when tested.

Furthermore, today's businesses are faced with increasingly complex web properties to protect. Hybrid public–private clouds are common with multiple vendor data centres around the world. Websites involve multi-level interactions with many device types including third-party software extensions, tracking objects, integrated advertising, social media plugins, real-time communication and chat bots. Sites are dynamic with multiple APIs to content engines and third-party interactions.

As a business with web assets to protect, how should you move forward?

What attendees will learn:

- Case study: review of the web application attack on British Airways
- The demise of the traditional WAF: blocking SQLi and OWASP top 10 threats is not enough
- How to keep control of data privacy with the disintegration of the 'network perimeter'
- A new approach to web application security: overview of the Oracle + Dyn Cybersecurity Suite

Education Seminars	
Osirium **How passwords get stolen, how attackers move laterally across networks, how to separate people from the passwords, how to add multifactor authentication to systems that don't natively support it** **Andy Harris,** Chief Technology Officer, Osirium	• The common methods of obtaining passwords, graded by how easy they are for an attacker to deploy • How password policies can be counter-productive and passwords vaults can be bypassed • How attackers move laterally across your network, and how to create enough friction to stop attackers but allow normal work to proceed • How different types of multifactor authentication work, how offline MFA can work, how to add multifactor authentication to systems that don't natively support it • Why task automation is so important to security
Pluralsight **The pace of change will never be this slow again – are you on the right side of disruption?** **Tommy Barlow,** Director EMEA, Pluralsight	For technology leaders and security professionals, disruption is the new normal. The pace of change is unprecedented and accelerating. New business models are putting pressure on companies to deliver innovation faster. And the competition for talent leaves a lot of teams understaffed and underskilled. To compete in this climate, you need to be able to reliably and predictably create technology skills at scale. Join us for a discussion on the disruption that's occurring and why you need to rethink the way you approach skills development. • How do you assess what technologies are trending in your industry/org? • How to evaluate who has what skills? • What is your strategy to reskill the workforce of today to meet the needs of tomorrow?