Post event report

e-crime & cybersecurity MID-YEAR

The 11th e-Crime & Cybersecurity Mid-Year Summit

17th October 2019 | London, UK

Strategic Sponsors

Attivo Networks

CrowdStrike

mimecast

OneTrust GRC
INTEGRATED RISK MANAGEMENT

SECUREDATA
PART OF ORANGE CYBERDEFENSE

SWIMLANE

virsec

zscaler

Education Seminar Sponsors

Accellion

AGARI

Blue Cube
Intelligent Protection

Cymulate
Breach & Attack Simulation

DIGITAL GUARDIAN

DEMISTO
A PALO ALTO NETWORKS COMPANY

illumio

NETACEA

netwrix

NOMINET

RED SIFT

RISKIQ

TREND MICRO

tripwire

Networking Sponsors

Cloud Control

illusive

ThreatConnect

Branding Sponsor

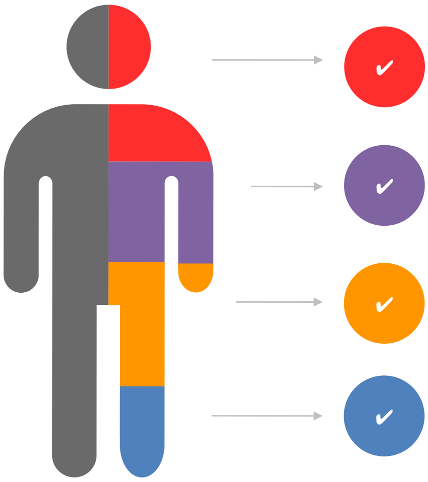
Cyber Security Project Works
INFOSECABILITY

> “The e-Crime Congress covers a variety of topics relevant to cybersecurity and risk management presented in well-controlled short sessions to keep the interests of the delegates piqued throughout the day. The education sessions and the opportunity to interact with the vendors and other delegates enables the attendees to supplement the knowledge gained in the main presentation. Hence e-Crime Congress is now on my list of favourite events to attend.”
>
> **IT Security & Risk Officer, UBS**

Key themes

- Let's talk about CISO overload
- Cybersecurity: someone else's problem?
- Cloud: not such a fluffy topic
- The people problem
- AI: much ado about nothing, or the only solution?
- Consolidating the security stack
- Joining up fraud, security and privacy

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

Tim Ager, VP Sales EMEA, Cymulate

Matt Arnull, Head of Enterprise Architecture, Arcadia Group

Liz Banbury, Head of Information & Cyber Policy, Standard Chartered Bank

Terry Bishop, Technical Director, EMEA, RiskIQ

Alex Booroff, Head of Information Security, Travelopia

Scott Bridgen, Offering Manager, GRC & Integrated Risk, OneTrust

Gabriel Dezon, Group Audit Manager, Technology, Dentsu Aegis Network

Dean Ferrando, Lead Systems Engineer, Tripwire

Kevin Fielder, CISO, Just Eat

Jim Hansen, President and COO, Swimlane

Ian Heritage, Security Architect, Trend Micro

Alphus Hinds, CISO, Standard Bank International

Mark Howell, VP UK & Ireland, Attivo Networks

Nick Ioannou, CSO, Ratcliffe Groves Partnership

Steve Jackson, Head of Financial Crime & MLRO, Covéa Insurance

Richard Kirk, Vice President EMEA, Illumio

Mark Langton, Director, Sales EMEA, Agari Data

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

Dave Matthews, Solutions Engineer, Netwrix

James Maude, Head of Threat Research, Netacea

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

Segun Oyinloye, Group CISO, Pepper Financial Group

Dan Panesar, Head of Sales EMEA, Nominet

Atiq Raza, Chairman & CEO, Virsec

Mark Ryan, Director, Product Management, Zscaler

Andy Shepherd, Sales Engineer, Demisto, A Palo Alto Networks Company

James Stevenson, Regional Sales Manager, Demisto, A Palo Alto Networks Company

John Titmus, Director, EMEA – Security Engineering, CrowdStrike

Mark Toshack, Senior Product Manager, Mimecast

Charl van der Walt, Chief Security Strategy Officer, SecureData

Steve Williamson, Audit Account Director, GSK

Harry Zorn, Vice President Sales, EMEA, Accellion

Agenda

08:00 Registration and breakfast networking

08:50 Chairman's welcome

09:00 **There is never a dull moment in cybersecurity...**

Steve Williamson, Audit Account Director, GSK

- Embedding foundation security controls, and providing assurance that they are operating effectively. Why this is now more important than ever, and how to manage increasing business demands and scrutiny
- New challenges due to legacy technologies and continual demands for greater automation
- Cyber-threats are recognised as a major business risk in most organisations, and the Board rely on the CISO (and internal Audit) to report this risk in meaningful business terms. It is unrealistic to expect an organisation to be 100% secure. How to report cyber-risk in a way which will allow the board to compare their risk exposure to their risk appetite
- Enabling the prioritisation of cybersecurity investment

09:20 **Automating incident response for SOC survival**

Jim Hansen, President and COO, Swimlane

- How a SOAR solution works: real-world use cases, including phishing, host alarms, endpoint detection and response
- How today's SOCs can use security orchestration, automation, and response (SOAR) solution to keep pace with the growing security skills gap and evolving threat landscape
- How SOAR solutions enable security operations teams to secure their organisations by doing more with less
- How SOARs empower the SOC by leveraging existing people, processes, and technology to investigate and remediate threats at machine speeds

09:40 **Defending against adversaries – what tactics can sport and warfare teach us to actively defend our networks from threat actors**

Mark Howell, VP UK & Ireland, Attivo Networks

- Tactics lessons from sport and warfare – what works when defending
- Honeypots – from science project to modern day deception
- Deception – attackers use it, defenders must
- How can we apply these tactics in the cyber-realm

10:00 **The unsustainable paradigm: are the business demands on today's ICS leader sustainable? How do you manage them?**

Liz Banbury, Head of Information & Cyber Policy, Standard Chartered Bank

- Is cyber too 'boring' for the cybersecurity professional? What skills does today's information security professional need? And why is it still so hard to find them?
- Information security policy and the relationship between policy and wider risk and business infrastructure
- Cybersecurity as a competitive advantage, especially in the financial services. How do you navigate/manage the demands of your clients/stakeholders? Comparative insights with other industries

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

Accellion	Cymulate	Illumio	Netacea	Tripwire
Protection in the age of the digital supply chain	**How to become APT-ready in four steps**	**Decoupling security segmentation from network infrastructure**	**Real or robot? The dangers of automated business logic attacks**	**Dissecting today's attacks to see the future of cybersecurity**
Harry Zorn, Vice President Sales, EMEA, Accellion	**Tim Ager,** VP Sales EMEA, Cymulate	**Richard Kirk,** Vice President EMEA, Illumio	**James Maude,** Head of Threat Research, Netacea	**Dean Ferrando,** Lead Systems Engineer, Tripwire

11:00 Refreshments and networking

11:30 **EXECUTIVE PANEL DISCUSSION** **Cyber-frenemies: why governance and audit may be security's greatest champions, and their biggest challenge**

Alex Blooroff, Head of Information Security, Travelopia
Gabriel Dezon, Group Audit Manager, Technology, Dentsu Aegis Network
Steve Jackson, Head of Financial Crime & MLRO, Covéa Insurance
Scott Bridgen, Offering Manager, GRC & Integrated Risk, OneTrust
Chaired by Segun Oyinloye, Group CISO, Pepper Financial Group

- The relationship between threat intelligence and overall corporate governance. Does good governance always equal good cybersecurity?
- What stake does internal audit hold in the security of your business? Can audit be security's biggest support?
- The increasing business demands on today's information security leader. Is it sustainable? And what – or who – can help?

11:50 **Every second counts: prioritising speed and security in the cloud era**

John Titmus, Director, EMEA – Security Engineering, CrowdStrike

In our modern world, speed often makes the difference between success and failure. This is equally true in the ever-evolving field of cybersecurity, where stealthy breaches can occur in a matter of hours, inflicting devastating consequences. Join John Titmus, Director, EMEA – Security Engineering at CrowdStrike as he explains the 1-10-60 concept and defines why these key outcome-driven metrics are critical to your organisation's security readiness. You will learn:

- Global 'breakout' time statistics, including observations on which adversaries showed the fastest tradecraft in the last 12 months
- Why speed of detection, investigation and remediation are key factors for successful day-to-day security management
- How Falcon Complete can fast-track your organisation to a 1-10-60 rule posture and elevate your cybersecurity maturity to the highest possible level, regardless of your internal resources

12:10 **Threat intelligence – how to stop bad things from happening to good organisations**

Mark Toshack, Senior Product Manager, Mimecast

- Human error
- Size of IT security teams
- Coping with influx of data

Agenda

12:30 Why understanding your attack surface matters

Charl van der Walt, Chief Security Strategy Officer, SecureData

- What does it mean to obtain and use 'cyber-intelligence' in a manner that effectively prioritises scarce resource across the full spectrum of 'Assess, Protect, Detect & Respond' cybersecurity disciplines?
- Threats in cyber-space arise for two main reasons: weakness in IT infrastructure and an interest taken by an attacker. Most businesses know they must mitigate cyber-threats for their own good but also because regulators require them to
- But the threat landscape is ever changing as technology evolves and attackers innovate. Ensuring an organisation has the skills, agility and underlying platforms and processes to understand, detect and manage cyber-threats is one of the most compelling challenges faced by any 21st century business. Regulatory changes have pushed the issue up to board level
- What should the priority be for an organisation that wants to improve its cybersecurity posture, finding and removing vulnerabilities in its infrastructure or assessing the external threats it faces?

12:50 Education Seminars | Session 2

Demisto, A Palo Alto Networks Company	Digital Guardian	Netwrix	Nominet	Red Sift
SOAR 101 – how would SOAR empower your SOC team?	**Comprehensive data protection combining DLP and EDR**	**Back to data security basics: what's getting lost in all the buzz**	**Getting ahead in the cloud**	**Time to fix your broken windows?**
James Stevenson, Regional Sales Manager, Demisto, A Palo Alto Networks Company, and **Andy Shepherd,** Sales Engineer, Demisto, A Palo Alto Networks Company	**Matt Logan,** Vice President of Field Engineering – EMEA, Digital Guardian	**Dave Matthews,** Solutions Engineer, Netwrix	**Dan Panesar,** Head of Sales EMEA, Nominet	**Rois Ni Thuama,** Head of Cybersecurity Governance & Legal Partnerships, Red Sift

13:30 Lunch and networking

14:30 Selling cyber to the C-suite. Making your business case to the right senior stakeholders

Nick Ioannou, CSO, Ratcliffe Groves Partnership

- Cyber accountability: what are the risks you are liable for?
- The increasingly varied and challenging role of the CISO. Today's CISO has 'around 8 jobs'! How does today's IT and information security leader juggle the various demands on them? How do you become sales negotiators, risk managers, technologists, trainers and mentors? And how does that impact resourcing of the next generation?
- Client questionnaires and navigating the demands of clients. How has this impacted the business/budget case for information security?
- Centralised security. Less than 50% of the Fortune 500 have a SOC. Is the idea of centralised security a pipe dream for most organisations? And how do you manage this with limited resources and budget?

14:50 The need for runtime security to defend against cyber-attacks

Atiq Raza, Chairman & CEO, Virsec

As global cyber-attacks and crime continue to proliferate, a new model is needed to protect critical applications and infrastructure from damage, disruption or worse. This presentation covers techniques attackers are using to bypass conventional security, and the urgent need to detect and stop attacks in real-time before damage is done. Topics will include:

- The increased sophistication of cybercriminals
- The shift to fileless and memory-based attacks
- The need to move beyond perimeter or after-the-fact security
- New technology to positively stop attacks during runtime

15:10 What is zero trust network access, and how can you achieve it?

Mark Ryan, Director, Product Management, Zscaler

- How you can transform your network from open access to a secure, policy-driven framework
- How to gain visibility of application access in a multi-cloud environment
- Keeping your users secure, no matter where they are or how they are connected

15:30 Education Seminars | Session 3

Agari Data	Illumio	RiskIQ	Trend Micro
How to fight cybercriminals that operate like businesses	**Decoupling security segmentation from network infrastructure**	**Defending your organisation and your customers against JavaScript injection attacks**	**Cyber-defence for cloud-first enterprise**
Mark Langton, Director, Sales EMEA, Agari Data	**Richard Kirk,** Vice President EMEA, Illumio	**Terry Bishop,** Technical Director, EMEA, RiskIQ	**Ian Heritage,** Security Architect, Trend Micro

16:10 Networking and refreshments

16:30 Grass-roots security from the ground up

Kevin Fielder, CISO, Just Eat

- How to build a cohesive cybersecurity strategy from the ground up
- Why are senior management, stakeholders and investors now paying attention to cybersecurity as a real business risk? What is at stake?
- How to create a business efficient cyber-risk framework
- Creating scalable cyber-infrastructure for an agile environment. How to manage digital evolution
- Case study: building grass roots security at Just Eat

16:50 Security and innovation – hand in hand or hand to throat?

Matt Arnull, Head of Enterprise Architecture, Arcadia Group

- How perceptions of security have changed, how engineering has changed
- The dangers of high-volume agile. Is agile innovation and security an unsustainable relationship?
- Solutions and key takeaways: how it's possible to have both – with examples from logistics, retail, hospitality and fashion

17:10 Keeping cyber simple. Are we over-complicating cybersecurity? And how can we simplify the problems, so we can get the right solutions?

Alphus Hinds, CISO, Standard Bank International

- The challenges of managing security at an international remit. What are the siloes, and cross-jurisdictional issues and risks that you need to take into account?
- The over-complexity of cybersecurity. Are we making cybersecurity more complicated than it needs to be? Is this affecting the communication of cybersecurity as a business risk to the board? And what can be done?
- The move to the Cloud. What do information security leaders need to take into account when it comes to accountability for Cloud security and dealing with CSPs?
- The evolving digitalisation of the financial services and how FinTech and open source platforms are changing the landscape of security. Are APIs the industry's worst nightmare?

17:30 Drinks reception

Education Seminars

Accellion

Protection in the age of the digital supply chain

Harry Zorn, Vice President Sales, EMEA, Accellion

The Accellion secure content communication platform helps IT executives lock down and govern the exchange of confidential enterprise information with the outside world without getting in the way of users. Thousands of global CIOs and CISOs trust Accellion to give their organisations protection, privacy and peace of mind.

- Third-party risk explained
- Protecting all communication channels of sensitive content
- Unify access to enterprise content silos without migration

Agari Data

How to fight cybercriminals that operate like businesses

Mark Langton, Director, Sales EMEA, Agari Data

Cybercriminals have figured out how to bypass our perimeter defences by targeting the most vulnerable part of any enterprise: the humans. They have also increased their success rates by 63% using identity-based email attacks.

Hear a story about how a Nigerian cyber-gang was exposed last December with extensive operations in the UK and Western Europe, who targeted 50,000 individuals during a five-month period. More than 70% of the victims were CFOs and the rest were finance leaders from companies of various sizes. This particular gang operated much like a modern corporation with members carrying out specific functions – everything from business intelligence, to lead generation and sales, which included the con itself.

Please join Mark Langton, Director of Sales at Agari as he exposes the inner workings of a sophisticated, UK-based cybercriminal organisation.

This session will shed light on:

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

Cymulate

How to become APT-ready in four steps

Tim Ager, VP Sales EMEA, Cymulate

With exposure rates showing that 70%–85% of organisations are vulnerable, advanced persistent threat (APT) groups' malware strains are no longer solely the worry of Fortune 1000 companies. When it comes to mature security departments, professionals are doing everything right. From perimeter security through DLP to encryption and segmentation – their practices are best practices. In terms of optimising their security posture, they're already 80% there. Yet big budgets don't translate into better security, and CISOs of large companies don't necessarily sleep better at night. So what is the 20%-equivalent of fine-tuning in the security world? What is the missing step to knowing you are truly secure from an APT attack?

Join us to learn:

- Key points in testing defensibility against APT attacks
- Where traditional security testing methods fall short of the mark
- How continuous visibility improves your cyber stance
- How empirical risk scores help you prioritise efforts and budget
- How you can become APT-ready in 4 steps

Education Seminars

Demisto, A Palo Alto Networks Company

SOAR 101 – how would SOAR empower your SOC team?

James Stevenson, Regional Sales Manager, Demisto, A Palo Alto Networks Company, and **Andy Shepherd,** Sales Engineer, Demisto, A Palo Alto Networks Company

Security teams face unique challenges in today's data-heavy landscape with sophisticated attackers and vast threat surfaces. As alert numbers rise and security product stacks grow, security teams struggle to execute standardised enrichment and response due to disparate tool sets, rising alert and false positive numbers, time-consuming manual actions, and human capital crunches. Teams need a tool stack that centralises security data, increases analyst productivity, and primes the SOC for scalable response.

This session will highlight how a Security Orchestration, Automation, and Response (SOAR) platform plugs in critical gaps in the incident response lifecycle. An in-depth demo will highlight how SOAR tools unify and automate actions across security products, structure processes through task-based workflows, and free up analyst time for important decision-making and deeper investigations.

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

- Coordinating actions across the entire security product stack
- Automating repeatable actions with human review and oversight
- Improving investigation quality by weeding out false positives
- Shaving down response times from hours to seconds

Attend the session and learn how a robust SOAR-powered incident response function is the first step to reduced security and business risk.

Digital Guardian

Comprehensive data protection combining DLP and EDR

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

As separate technologies DLP and EDR excel at protecting your data and stopping threats. Combined they are a formidable force providing complete end to end visibility of how external influences breach your organisation and target data to exfiltrate. With one combined solution you can stop, block and keep your assets and data in your control.

What attendees will learn:

- Importance of data visibility for DLP
- How data classification enhances the EDR capacity
- How Digital Guardian detects, prioritises and remediates both internal and external threats in a single agent

Illumio

Decoupling security segmentation from network infrastructure

Richard Kirk, Vice President EMEA, Illumio

Malware, ransomware and other cybercrime attacks are growing and becoming more sophisticated. And yet many businesses are not prepared to protect themselves from the inherent risks and dangers. This is often because most internal networks are wide open by design, since using traditional data centre firewalls as a security measure is difficult and expensive. Would you like to learn about a new way to decouple security segmentation from the network infrastructure, and implement an affordable, practical way to protect your business?

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

Education Seminars

Netacea

Real or robot? The dangers of automated business logic attacks

James Maude, Head of Threat Research, Netacea

When organisations consider how to protect their web applications from attacks, they often focus on security scans and pen tests to identify technical security flaws. While this is absolutely correct, another risk often remains undetected until it's too late: business logic attacks.

These use legitimate application functionality, built to enable your customers to use your product or service, to bypass traditional defences and test stolen credentials, steal data and commit fraud. As rising levels of automation in online attacks make it easier than ever for malicious visitors to look like real users and target an organisation's unique business logic, it's critical to understand this evolving threat.

Attendees will learn:

- The key challenges businesses face in protecting against automated attacks
- Real-world examples of how organisations are being attacked
- The limitations of existing mitigation techniques
- How attackers are reverse-engineering your defences
- How to evaluate the risks and build better defences

Netwrix

Back to data security basics: what's getting lost in all the buzz

Dave Matthews, Solutions Engineer, Netwrix

As data usage grows exponentially, many organisations are struggling with information security because they are short on time, money, staffing or all of the above.

At the same time, the buzz from vendors about the latest attack vectors makes data security appear more complicated than it needs to be. This never-ending pursuit of defence against the hottest threats leads organisations to neglect basic aspects of data security, such as realising that not all data requires the same level of protection.

In this session, we'll explain how getting back to basics can strengthen security controls and reduce the risk of breaches.

Nominet

Getting ahead in the cloud

Dan Panesar, Head of Sales EMEA, Nominet

Adoption of cloud computing has been slow given the need to relinquish control of systems and data to third parties. Security-based concerns are being overcome, but how can cloud drive innovation at your organisation? Join Dan Panesar, Head of Sales EMEA at Nominet, as he considers uptake of the cloud in enterprises and the public sector.

- How the perception of cloud – from both an adoption and security perspective – is changing
- Cloud risk; hybrid, multi-cloud and on-premise
- How cloud can become a security enabler
- Staying secure through cloud transition and broader digital transformation

Red Sift

Time to fix your broken windows?

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

In the 80s, New York police commissioner Bill Bratton implemented the famous zero-tolerance policy based on the 'Broken Windows' theory to great effect. This session will explore how this real-world approach to fighting crime can be successfully adapted and applied to a law firm's virtual world to ensure a robust approach to cybersecurity.

- The session will start by looking at the Broken Windows theory in more detail
- It will then move onto looking at two of the tactics that 'traditional' criminals use to good effect to identify their victims
- Dig into the effective policing methods, including the zero-tolerance policy, that was employed to combat crime
- Finally, Rois will unpick these lessons and apply them to the cyber world to help others build a robust approach to cybersecurity

Education Seminars

RiskIQ

Defending your organisation and your customers against JavaScript injection attacks

Terry Bishop, Technical Director, EMEA, RiskIQ

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

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

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

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

Trend Micro

Cyber-defence for cloud-first enterprise

Ian Heritage, Security Architect, Trend Micro

Security is often misunderstood and addressed in the last stages of a project. Operationally, it's ignored until there is an emergency. This session outlines why security automation and consolidation will help realise your digital transformation quicker. This approach helps you and your team increase your security while reducing the overall operational overhead. Leave this talk with everything you need to start automating security.

- How to realise digital transformation earlier
- How to increase security whilst reducing the operational overhead

Tripwire

Dissecting today's attacks to see the future of cybersecurity

Dean Ferrando, Lead Systems Engineer, Tripwire

Dissecting the current threat landscape and analysing major data breaches from the last decade, this session explores how these insights can help us predict the future of cybersecurity. We'll look at the key factors that many high-profile breaches have in common, and why cybercriminals continue to leverage tried-and-tested tactics to be successful in their attacks.

Attendees will learn the emerging trends shaping the future state of cybersecurity, and what foundational controls, industry frameworks and resources organisations can use today to better prepare for tomorrow's threats.

In this session you will:

- Learn about the key factors many high-profile breaches have in common
- Understand the emerging trends shaping the future state of cybersecurity
- Understand what foundational controls to use today to bolster your cybersecurity strategy
- Understand how employee education can help reduce the success of cyber-attacks
- Learn about resources and industry frameworks to help strengthen your overall security posture
- How to start processing security automation