Post event report

The 11th e-Crime & Cybersecurity Congress in Abu Dhabi
17th September 2019 | Abu Dhabi, UAE

"Very well organised and pleasant to attend from the beginning till end. The seminar exceeded my expectations in terms of AML cybercrime threats and how to deal with it. I have a complete new understanding of cybersecurity, innovation and technologies. All presenters were really knowledgeable and gave us amazing information in only 20 minutes. It was a terrific use of my time. Thank you very much!"
AML and Compliance Officer
Lari Exchange

"It is a pleasure to attend every year to network and to learn more about the cybersecurity world. It was so beneficial to be honest and I will be glad to provide a testimonial from my side."
Manager Security Compliance
DU

"Once again It was my pleasure to be part of e-crime conference. I am looking forward the next one in Dubai in March 2020."
Head of Fraud Investigations,
Risk Management
RakBank

Inside this report:
Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars
Key themes

Dealing with nation-state actors and exploits

Compliance with new regulations

Innovation + security: friends or foes?

Coping with a runaway threatscape

Who’s who? Improving identity analytics

In or out?

Who attended?

Speakers

Ashraf Aboukass, Global Head of Information Security Architecture, Schroders
Muhammad Babar, Head of Compliance, Moneygram International
Oussama Bachour, Senior Systems Engineer, Fortinet
Jerome Bei, Sales Engineering Manager, EMEA, Accellion
Jerry Peter Bruzzese, Microsoft MVP (Office Apps and Services), Mimicast
Robert Cookson, Group IT Director, NOW Health International
Phillip Davies, Director of Anti-Piracy, Sky
Richard Davis, Cyber Security Strategist EMEA, Proofpoint
Justin Doo, Territory Manager Middle East, Turkey & Africa, Okta
Astrid Hansen, Chief Controls Officer and Head of Information Security, MENA, Barclays
Kamel Heus, Regional Director, EMEA South & MEA, Centrify
Bahi Hour, SE Director, META, Attivo Networks
Ahmed Husain, CEO, Reload, on behalf of Protection Group International
Ilham Ismail, Head of IT, Hospitality Management Holdings
Shafiullah Mohamed Ismail, Senior Manager, Security Architect & IT Governance, Mubadala Development Company
Ashish Khanna, Group Information Security Officer, Dubai Health Authority
Sebastian Madden, Chief Corporate Development Officer, Protection Group International
John Manning, former Head of Technology Risk, Prudential
Andrew March, Platform Specialist, EMEA, Okta
Richard Meeus, Security & Strategy Director EMEA, Akamai Technologies
Rebekah Moody, Market Planning Director, ThreatMetrix
Kausar Mukri, Head of Information Security, InvestBank
Suresh Nair, Chief Information Security Officer – MENAT, GE
Ronaldus Peeters, Managing Director EMEA, Synack
Matthew Platten, Anti-Fraud Solutions Consultant, Cyxtera
Muhammad Rizwan Khan, Head of Compliance, Aldhabab Exchange
Amit Roy, EVP and Regional Head of EMEA, Paladion Networks
Hashim Saeed, Head of Information Technology, Azizi Developments
Emile Abou Saleh, Regional Leader – Middle East, Turkey & Africa, Proofpoint
Martin Sivorn, Head of Cybersecurity, UK Government Digital Service
Nicolai Solling, Chief Technology Officer, Help AG
Jason Steer, Director of EMEA Presales, Recorded Future
Paul Steiner, Managing Director EMEA Sales, Accellion
Roland Stride, Director, Darktrace
Dr. Aleksandar Valjarevic, Head of Solution Architecture, Help AG
Jose Varghese, EVP and Head Of MDR Services, Paladion Networks
Emile Witte, Senior Product Marketing Manager Security EMEA, Akamai Technologies
Michael Yeardley, Senior Director, Product Strategy, ThreatMetrix
## Agenda

### 08:00 | Registration

### 08:50 | Chairman’s welcome, Amanda Oon, Deputy Editor, AKJ Associates, Soizic le Leslé Fauvelle, Conference Producer, AKJ Associates, and Robert Walker, Managing Director, AKJ Associates

### 09:00 | The new wave of AI/ML cyber-attacks

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

### 09:20 | A global view of cybercrime threats: it takes a network to fight a network

- **Michael Yeardley**, Senior Director, Product Strategy, ThreatMetrix, and Rebekah Moody, Market Planning Director, ThreatMetrix
  - Latest global trends as seen in the ThreatMetrix Digital Identity Network, based on analysis from 16bn transactions seen globally in H1 2019
  - How harnessing the power of that Network can establish Trust, Confidence, and Integrity
  - With practical insight into how that Network can be used to detect advanced fraud, protect consumers and support digital transformation

### 09:40 | Bestsellers in the underground economy: measuring malware popularity by forum

- **Jason Steer**, Director of EMEA Presales, Recorded Future
  - How the majority of the top 10 mentions of malware in multiple languages included openly available dual-use tools, open-source malware, or cracked malware
  - How many key malware families are over three years old or can be mitigated with basic security precautions
  - How activity in underground forums correlates to growth in malware in the real world

### 10:00 | Playing by the rules (and regulations). Managing your relationship with regulators and other security stakeholders

- **Astrid Hansen**, Chief Controls Officer and Head of Information Security, MENA, Barclays
  - The roles and influence of regulators and how that has changed over the last few years
  - The increased prioritisation of FS regulators such as the UAE Central Bank towards data governance and digital compliance
  - The cross-jurisdictional comparisons in a global organisation
  - The scrutiny of B2B clients towards information security and data governance. What are their demands and how can information security work as a commercial competitive advantage?

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

<table>
<thead>
<tr>
<th>Accellion Protection in the age of the digital supply chain</th>
<th>Cyxtera Digital risk protection to enhance user experience</th>
<th>Fortinet WAN edge security posture in the SD-WAN era</th>
<th>Help AG FILES: The enfant terrible of any IT environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jerome Bei, Sales Engineering Manager, EMEA, Accellion, and Paul Steiner, Managing Director EMEA Sales, Accellion</td>
<td>Matthew Platten, Anti-Fraud Solutions Consultant, Cyxtera</td>
<td>Oussama Bachour, Senior Systems Engineer, Fortinet</td>
<td>Nicolai Solling, Chief Technology Officer, Help AG, and Dr. Aleksandar Valjarevic, Head of Solution Architecture, Help AG</td>
</tr>
</tbody>
</table>

### 11:00 | Morning break

### 11:30 | Cyber-economics: information security metrics and incentives

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

### 11:50 | Deception-based threat detection myths & realities – changing the game on modern-day attackers

- **Bahi Hour**, SE Director, META, Attivo Networks
  - The challenge of current cyber threat dwell time – detection gap shift from cyber-threat prevention to innovative detection and incident response
  - The need for deception
  - How it works
  - Myths and realities – common misconceptions

### 12:10 | Prevent, respond and recover: email security priorities for 2020 cyber-resilience

- **Jerry Peter Bruzzese**, Microsoft MVP (Office Apps and Services), Mimecast
  - Develop your defence-in-depth strategy (email, web, awareness training)
  - Evaluate the connection between security and continuity: human error and the real risks of downtime

### 12:30 | Shift to self-learning, self-defending networks

- **Roland Stride**, Director, Darktrace
  - Leveraging AI algorithms to defend against advanced, never-seen-before, cyber-threats
  - How new immune system technologies can provide 100% visibility of your entire business, and enable you to pre-empt emerging threats & reduce incident response time
  - Why autonomous response is enabling security teams to neutralise in-progress attacks, prioritise resources, and tangibly lower risk
  - Real-world examples of subtle, unknown threats that routinely bypass traditional controls
Agenda

12:50 Education Seminars | Session 2

| 12:50 | Akamai Technologies | Centrify | Okta | Protection Group International
| --- | --- | --- | --- | ---
| | No. It really IS all about you… Identity | Anatomy of a hack: Perception vs. Reality | Customers in the crosshairs | Ditch the SOC, build a fusion centre
| | – use/abuse/compliance | Kamel Heus, Regional Director, EMEA South &MEA, Centrify | Andrew March, Platform Specialist, EMEA, Okta, and Justin Doo, Territory Manager Middle East, Turkey & Africa, Okta | Ahmed Husain, CEO, Reload, on behalf of Protection Group International
| | Richard Meeus, Security & Strategy Director EMEA, Akamai Technologies, and Elmar Witte, Senior Product Marketing Manager Security EMEA, Akamai Technologies | | |

13:30 Lunch break

14:30 The core issues of innovation and new technologies

Muhammad Rizwan Khan, Head of Compliance, Aldahab Exchange
- New innovation and smart technologies can be very effective tools to mitigate the risk of money laundering and terrorist financing for FI. How can you use them most effectively?
- The ROI of corporate awareness and training. What is required specially in FIs, regarding how to protect information and how cybersecurity can be applied through advanced solutions that may relax the business and employees in a secure environment?
- Effective framework must cover the scope of cyber-risk management and identify the gaps from IT to compliance that will be mutually beneficial for the company. How do you combine different functions such as cybersecurity and audit in an effective risk framework?

14:50 The confidence game: how attackers exploit people, and how to stop them

Richard Davis, Cyber Security Strategist EMEA, Proofpoint, and Emile Abou Saleh, Regional Leader – Middle East, Turkey & Africa, Proofpoint
- Learn how to identify who’s being attacked in your organisations; many organisations have little idea which of their people receive sophisticated threats, targeted threats or even large volume threats. We call these target VAPs (Very Attacked People) – they are not who you would expect
- Discuss how to leverage data to better understand your adversaries; phishing and social engineering are the ways most organisations get compromised
- Learn how to tailor a protection plan for your most at risk people

15:10 Why the best laid cybersecurity plans fail, and what you can do about it today

Jose Varghese, EVP and Head Of MDR Services, Paladion Networks, and Amit Roy, EVP and Regional Head of EMEA, Paladion Networks
- In this session, we will cover the three critical components you need in your cybersecurity programme
- To detect and respond to threats faster
- The time it could take your organisation to develop these capabilities
- The steps CISOs or security leaders can take to build this system and culture in their organisation

15:30 Digital piracy, a global cybercrime: let’s take the fight to the pirates

Phillip Davies, Director of Anti-Piracy, Sky
- Piracy as a trans-national, borderless issue. How can we explore the issues of regulating and navigating digital crime in a borderless business world?
- How has this been impacted by the onset of digitalisation and the race towards hyper-connectivity?
- APls, PayPal and cryptocurrency. Are these just buzzwords, or have they changed the way we – and the cybercriminals – manage digital fraud?
- What does today’s fraud leader need to know?

15:50 How offensive security testing better protects you against malicious hackers and nation state-sponsored cyber-attacks

Ronaldus Peeters, Managing Director EMEA, Synack
- There is continued, rapid growth in cyber-attacks and these are increasingly sophisticated with greater break-in success
- Traditional vulnerability scanning and compliance-based penetration testing prove ineffective in detecting many serious vulnerabilities in live systems
- Hear about a new revolutionary security testing approach using large teams of highly vetted international, top-class security researchers who can find serious vulnerabilities in any live system often within a matter of hours
- Several supporting case studies are discussed including how Synack was able to break into the Pentagon within just four hours

16:30 EXECUTIVE PANEL DISCUSSION

| 16:30 | Know your cyber-stakeholders. Insights into who has accountability in your organisation for cybersecurity. And what they’re doing about it | Chaired by: Amanda Oon, Deputy Editor, AKJ Associates
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Muhammad Babar, Head of Compliance, Monegram International</td>
<td>Robert Cookson, Group IT Director, NOW Health International</td>
</tr>
<tr>
<td></td>
<td>Robert Cookson, Group IT Director, NOW Health International</td>
<td>Suresh Nair, Chief Information Security Officer – MENAT, GE</td>
</tr>
<tr>
<td></td>
<td>Suresh Nair, Chief Information Security Officer – MENAT, GE</td>
<td>Shafiiulah Mohomed Ismail, Senior Manager, Security Architect &amp; IT Governance, Mubadala Development Company</td>
</tr>
</tbody>
</table>

16:50 Achieving ‘the impossible’: cybersecurity and controlled spending

Sebastian Madden, Chief Corporate Development Officer, Protection Group International
- Introduction to the Organisational Cybersecurity Maturity Assessment Model
- Application to typical cybersecurity functions and units
- Regulatory alignment to national and sectoral standards
- Using the maturity model to identify over-investment, under investment and ineffective spend

17:10 EXECUTIVE PANEL DISCUSSION

| 17:10 | Lessons on dealing with digitalisation | Chaired by: Amanda Oon, Deputy Editor, AKJ Associates
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ilham Ismail, Head of IT, Hospitality Management Holdings</td>
<td>Kausar Mukeri, Head of Information Security, InvestBank</td>
</tr>
<tr>
<td></td>
<td>Kausar Mukeri, Head of Information Security, InvestBank</td>
<td>John Manning, former Head of Technology Risk, Prudential</td>
</tr>
<tr>
<td></td>
<td>John Manning, former Head of Technology Risk, Prudential</td>
<td>Hashim Saeed, Head of Information Technology, Azizi Developments</td>
</tr>
<tr>
<td></td>
<td>Hashim Saeed, Head of Information Technology, Azizi Developments</td>
<td>Ashish Khanna, Group Information Security Officer, Dubai Health Authority</td>
</tr>
</tbody>
</table>

17:30 Conference close. Robert Walker, Managing Director, AKJ Associates
## Education Seminars

### Accellion
**Protection in the age of the digital supply chain**
Jerome Bei, Sales Engineering Manager, EMEA, Accellion, and Paul Steiner, Managing Director EMEA Sales, 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
- Zero trust – a viable strategy?
- Protecting all communication channels of sensitive content
- Unify access to enterprise content silos without migration

### Akamai Technologies
**No. It really IS all about you… Identity – use/abuse/compliance**
Richard Meeus, Security & Strategy Director EMEA, Akamai Technologies, and Elmar Witte, Senior Product Marketing Manager Security EMEA, Akamai Technologies

Cybercrime revolves around users and users rely on their identities. Protecting the identity of your customers will help you to protect your brand against the next breach.

Join Akamai on this educational seminar where we will discuss how cybercriminals are abusing password reuse, exploiting VPN tunnels and searching for soft targets.

- Learn on techniques to detect and prevent credential stuffing
- See how to minimise the attack surface when machines or users are compromised
- Ensure that all your assets are protected, not just the shiny website

### Centrify
**Anatomy of a hack: Perception vs. Reality**
Kamel Heus, Regional Director, EMEA South & MEA, Centrify

The number of data breaches has skyrocketed in recent years. Contrary to popular belief and Hollywood story lines, cyber-attacks are rarely carried out by legions of highly sophisticated coders gone rogue, deploying the most advanced techniques to penetrate organisations’ perimeter defences. Reality paints a very different picture: cyber adversaries are no longer hacking to carry out data breaches – they’re simply logging in by exploiting weak, stolen, or otherwise compromised credentials. Implementing an effective enterprise security strategy requires an understanding of hackers’ tactics, techniques, and procedures – often called TTPs.

This breakout session will provide not only insight into the latest tactics, techniques, and procedures used by cyber-adversaries, but more importantly provide best practices on how to implement a successful cybersecurity strategy in organisations, independent of their size and industry.

The session will cover:

- The anatomy of a hack
  - Common misconceptions
  - Today’s TTPs and cyber-attack lifecycle
- A blueprint on how to minimise your risk exposure
  - Best practices revealed
  - Meet the antidote: zero trust
  - The path to zero trust starts with identity
  - Real-life implementation examples

### Cyxtera
**Digital risk protection to enhance user experience**
Matthew Platten, Anti-Fraud Solutions Consultant, Cyxtera

In a digital-first world where more and more users rely on online banking, financial losses to cybercrime have increased by over 40% in the past three years. Adding insult to injury, end users expect the highest level of security from their banking provider and won’t tolerate protection that only applies after their account has been compromised.

Join Cyxtera as we’ll cover the following topics to help find the right risk protection balance:

- The state of external threats and customer expectations
- The downfalls of only a reactive risk mitigation strategy
- How to balance the scales with proactive threat detect and response
<table>
<thead>
<tr>
<th><strong>Education Seminars</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fortinet</strong></td>
</tr>
<tr>
<td><strong>WAN edge security posture in the SD-WAN era</strong></td>
</tr>
<tr>
<td>Oussama Bachour, Senior Systems Engineer, Fortinet</td>
</tr>
<tr>
<td>This session discusses the importance of security for a complete WAN edge transformation from headquarters to the enterprise branch. The presentation includes use cases and real-world examples of how organisations are using Secure SD-WAN to empower the workforce globally.</td>
</tr>
<tr>
<td>• Overview of challenges and complexity of existing and legacy enterprise WAN edge networks</td>
</tr>
<tr>
<td>• The impact of digital transformation on the design and requirement of enterprise WAN edge</td>
</tr>
<tr>
<td>• SD-WAN drivers and embedded technologies as solution for WAN edge transformation</td>
</tr>
<tr>
<td>• Mitigation of security risks incorporated during digital transformation and the adoption of SD-WAN systems</td>
</tr>
<tr>
<td>• Use cases and real-world examples from customers’ deployments</td>
</tr>
<tr>
<td><strong>Help AG</strong></td>
</tr>
<tr>
<td><strong>FILES: The enfant terrible of any IT environment</strong></td>
</tr>
<tr>
<td>Nicolai Solling, Chief Technology Officer, Help AG, and Dr. Aleksandar Valjarevic, Head of Solution Architecture, Help AG</td>
</tr>
<tr>
<td>• There are thousands of file formats and they are ultimately the agents that deliver everything from a website to an attachment in your inbox. While files are good and deliver functionality, they can also be bad, weaponised delivery vehicles for malware</td>
</tr>
<tr>
<td>• In this session we will talk about files, the types one should be extra careful about and how these are utilised in social engineering malware and crypto-attacks</td>
</tr>
<tr>
<td>• In a world where attackers have more resources and capabilities than ever, we will discuss how small changes and new technology can significantly increase your robustness against both file-based and file-less attacks</td>
</tr>
<tr>
<td><strong>Okta</strong></td>
</tr>
<tr>
<td><strong>Customers in the crosshairs</strong></td>
</tr>
<tr>
<td>Andrew March, Platform Specialist, EMEA, Okta, and Justin Doo, Territory Manager, Middle East, Turkey &amp; Africa, Okta</td>
</tr>
<tr>
<td>As users now expect more from the organisations they interact with online, managing the identity of your customers is becoming much more complex. Password dumps, multiple devices and poor MFA adoption put pressure on security and development teams. All the time your competition is waiting in the wings ready to offer an alternative if your offering doesn’t meet the customer’s expectations.</td>
</tr>
<tr>
<td>Join Andy in a session where he discusses the threats to your customers, the impact those threats can have on your organisation and how to build a customer identity that not only protects your customers but provides a better user experience.</td>
</tr>
<tr>
<td><strong>What attendees will learn:</strong></td>
</tr>
<tr>
<td>• How to model the risks and impacts of a customer account compromise</td>
</tr>
<tr>
<td>• How to drive registration with progressive profiling</td>
</tr>
<tr>
<td>• Choosing multifactor options that users love</td>
</tr>
<tr>
<td>• Techniques for monitoring emerging account threats</td>
</tr>
<tr>
<td><strong>Protection Group International</strong></td>
</tr>
<tr>
<td><strong>Ditch the SOC, build a fusion centre</strong></td>
</tr>
<tr>
<td>Ahmed Husain, CEO, Reload, on behalf of Protection Group International</td>
</tr>
<tr>
<td>What you need is a SOAR powered cyber-threat management and response centre. The SOC or the Cyber Command should be equipped with real-time strategic, tactical and operational threat intelligence and cyber data fusion capabilities to produce a 360-degree view of an adversary. This approach empowers organisations to effectively combat threats by collecting, visualising and correlating reliable threat data from multiple trusted tools and sources and delivering an automated threat response.</td>
</tr>
<tr>
<td>In this session, attendees will learn:</td>
</tr>
<tr>
<td>• How to map your incidents and intelligence to the MITRE Att&amp;ck framework and help your threat hunter in prioritising what to hunt and where to hunt</td>
</tr>
<tr>
<td>• How to collect reliable threat intelligence data and employ it to the best business advantage</td>
</tr>
<tr>
<td>• How to achieve 360 degree visibility with SOAR powered threat management</td>
</tr>
</tbody>
</table>