

# Post event report



The 10<sup>th</sup> e-Crime & Cybersecurity Congress in Abu Dhabi

19<sup>th</sup> September 2018 | Abu Dhabi, UAE

Principal Sponsor



Strategic sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsors



“ It was great to participate in the e-Crime & Cybersecurity Congress in Abu Dhabi on the 19<sup>th</sup> September 2018. The congress was very informative, the topics were interesting, and there was a wide variety of vendors. ”

Senior IS Auditor,  
State Audit Institution

“ It was a fantastic experience attending the 10<sup>th</sup> e-Crime & Cybersecurity Congress in Abu Dhabi. As usual, e-Crime exceeded our expectations. The presentations have always been refreshing, realistic and updated according to the current trends on how to mitigate the risk of cybercrime. ”

IT Manager,  
Al Muqren Exchange

“ It was a really great event. Everything was perfect starting from the registration and presentation timings until the closing of the event. ”

Senior Officer IT Security,  
Daman

Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars



### Speakers

- Abishek Surendra Babu, IT Security Specialist, **ManageEngine**
- Amit Bhatia, Head of Information Security, **major financial institution**
- Kalle Björn, Director, Systems Engineering – Middle East, **Fortinet**
- Simon Brady, Managing Editor, **AKJ Associates**
- Brian Byagaba, Head of Information Security, **Commercial Bank International**
- John Cassidy, Global Sales Leader, **Ground Labs**
- Hariprasad Chede, Chief Information Security Officer, **National Bank of Fujairah**
- Ozgur Danisman, Sr. Engineer Manager, Middle East and North Africa, **Forcepoint**
- Simon Davey, Senior Business Development Executive, **Ground Labs**
- Tamer El Refaey, Business Development Manager, Enterprise Security, **Micro Focus**
- Elizabeth de Freitas, Regional Manager, **Darktrace**
- Nour Fateen, Pre-Sales Consultant, **Recorded Future**
- Nicolas Fischbach, Global Chief Technology Officer, **Forcepoint**
- Angharad Gilbey, Content Production Executive, **AKJ Associates**
- Michael Hirschfeld, Cyber Security Advisor, **SABSAcourses**
- Ahmed Husain, CEO, Reload, on behalf of **Protection Group International**
- Shafique Ibrahim, Group Head of IT, **Al Fardan Group**
- Ilham Ismail, Head of IT, **Hospitality Management Holdings**
- Adam Lalani, Group Head of IT, **Tristar Transport**
- Sebastian Madden, Chief Corporate Development Officer, **Protection Group International**
- Mohamad Makhzoum, Cyber Security Specialist, **Juniper Networks**
- Scott Manson, Leader of Middle East, **McAfee**
- Simon Moores, Director, **Zentelligence**
- Siddhartha Murthinty, Security Solutions Architect, **Spire Solutions**
- Mahdi Naili, Senior Systems Engineer, **Fortinet Middle East**
- Dennis Oommen, Technical Head, **Spire Solutions**
- Paolo Passeri, Solutions Architect, **Netskope**
- Ashfak Pathan, Senior Security Consultant, **Spire Solutions**
- Hamid Qureshi, Territory Sales Manager, **Thales**
- Christopher Rollan, Head of IT, **GOPA-intec**
- Abbas Sabuwala, Head of Information Security and Support Systems, **United Arab Shipping** (subsidiary of Hapag Lloyd)
- Vibin Shaju, Director of Pre-Sales Southern Europe & MET, **McAfee**
- Nicolai Solling, Chief Technology Officer, **Help AG Middle East**
- Anshul Srivastav, Chief Information and Digital Officer, **Union Insurance**
- Dr. Aleksandar Valjarevic, Head of Solution Architecture, **Help AG**
- Robert Walker, Managing Director, **AKJ Associates**
- Michael Yeardeley, Senior Director, Product Strategy, **ThreatMetrix**

### Key themes

- When state-actors are the main threat
- Machine learning and AI
- Rise of the robots?
- Blockchain - hype versus reality
- Understanding the Cloud: the devil is in the detail
- Keeping up with the regulators

### Who attended?



Agenda					
08:00	Registration and breakfast networking				
08:50	Chairman's welcome by <b>Simon Brady</b> , Managing Editor, AKJ Associates, and <b>Robert Walker</b> , Managing Director, AKJ Associates				
09:00	<b>Who secures the UAE? The end-user verdict on vendors</b>				
	<p><b>Simon Brady</b>, Managing Editor, AKJ Associates, and <b>Angharad Gilbey</b>, Content Production Executive, AKJ Associates</p> <ul style="list-style-type: none"> <li>Who do UAE companies choose for cybersecurity and why?</li> <li>What makes cyber-risk management here different?</li> <li>What are the key challenges facing UAE cybersecurity professionals?</li> </ul>				
09:20	<b>Help! I'm only as strong as my weakest 3rd party!</b>				
	<p><b>Dennis Oommen</b>, Technical Head, Spire Solutions</p> <ul style="list-style-type: none"> <li>In an increasingly 'connected' business world, how can you effectively measure and manage 3rd party cyber-risk?</li> <li>When you can't 'see' inside your partner/3rd party organisations, how do you gauge their 'cyber-health'?</li> <li>How do you provide your leadership with an independent assessment of your own external security posture and benchmark against industry peers?</li> </ul>				
09:40	<b>Leveraging AI for dynamic and surgical autonomous response for cyber-defence, with learnings from The City of Las Vegas</b>				
	<p><b>Elizabeth de Freitas</b>, Regional Manager, Darktrace</p> <ul style="list-style-type: none"> <li>Insight into how AI can be applied to close the time between threat detection and response, and counter activity of malicious threats</li> <li>Understanding the evolving pattern of normality within a network, which can be discerned through machine learning</li> <li>Using surgical autonomous response and containment of only the most relevant threats, to limit the interruption of normal business and employee activity</li> <li>Applying AI to augment the capability of human security teams, undermining the myth that AI will replace human operators</li> </ul>				
10:00	<b>Extending behavioural insights to drive risk adaptive protection and enforcement</b>				
	<p><b>Nicolas Fischbach</b>, Global Chief Technology Officer, Forcepoint, and <b>Ozgur Danisman</b>, Sr. Engineer Manager, Middle East and North Africa, Forcepoint</p> <ul style="list-style-type: none"> <li>Today's behaviour analytics tools provide insights into risky and anomalous activity but most are powerless as unable to enforce protection policies</li> <li>How insights on risky human behaviour and abnormal activity can be gained by tightly integrating user and entity behavioural analytics (UEBA) with other security technologies</li> <li>How to break free of the forensic nature of UEBA's, protecting data and user insights with policy enforcement to happen as security events occur</li> </ul>				
10:20	<b>Education Seminars   Session 1</b>				
	<p><b>Ground Labs</b> <b>Standards don't bother me – all I want is your data!</b> <b>John Cassidy</b>, Global Sales Leader, Ground Labs, and <b>Simon Davey</b>, Senior Business Development Executive, Ground Labs</p>	<p><b>PGI</b> <b>Chasing the dream of the clean pipe: where are we today?</b> <b>Ahmed Husain</b>, CEO, Reload, on behalf of Protection Group International</p>	<p><b>Recorded Future</b> <b>The dark web's deep threat intelligence secrets</b> <b>Nour Fateen</b>, Pre-Sales Consultant, Recorded Future</p>	<p><b>Spire Solutions</b> <b>Attack is the best form of defence!</b> <b>Siddhartha Murthinty</b>, Security Solutions Architect, Spire Solutions</p>	<p><b>ThreatMetrix</b> <b>Digital identities, consumer identities and beyond...</b> <b>Michael Yeardley</b>, Senior Director, Product Strategy, ThreatMetrix</p>
11:00	Networking and refreshments break				
11:30	<b>Ransom on the high seas</b>				
	<p><b>Abbas Sabuwala</b>, Head of Information Security and Support Systems, United Arab Shipping (subsidiary of Hapag Lloyd)</p> <ul style="list-style-type: none"> <li>The next hacker playground: the open seas – and the oil tankers and container vessels that ship 90% of the goods moved around the planet</li> <li>As more devices are hooked up online, so they become more vulnerable to attack</li> <li>As industries like maritime and energy connect ships, containers and rigs to computer networks, how they expose weaknesses that hackers can exploit</li> </ul>				
11:50	<b>The rise of the cloud threats</b>				
	<p><b>Paolo Passeri</b>, Solutions Architect, Netskope</p> <ul style="list-style-type: none"> <li>How the cloud is influencing the threat landscape</li> <li>Real-world campaign examples</li> <li>How to embrace the journey to the cloud in a secure manner</li> </ul>				
12:10	<b>Lessons learned: building an insider threat programme</b>				
	<p><b>Tamer El Refaey</b>, Business Development Manager, Enterprise Security, Micro Focus</p> <ul style="list-style-type: none"> <li>What to consider when building a successful insider threat programme</li> <li>Technologies that can help in building a successful insider threat programme</li> <li>How a SOC can support the insider threat programme</li> <li>How a successful insider threat programme can help protect organisations from external cyber-attacks</li> </ul>				

Agenda					
12:30	<b>EXECUTIVE PANEL DISCUSSION</b> <b>Cybersecurity training and tackling the skills shortage</b> Chaired by: <b>Simon Moores</b> , Director, Zentelligence <b>Amit Bhatia</b> , Head of Information Security, major financial institution <b>Sebastian Madden</b> , Chief Corporate Development Officer, Protection Group International <b>Mansoor Mughal</b> , Information Security, Dubai Financial Market <b>Christopher Rollan</b> , Head of IT, GOPA-intec				
12:50	<b>Education Seminars   Session 2</b>				
	<b>Juniper Networks</b> <b>The 101 on SDN: why software-defined secure networks are changing the industry and what you need to know</b> <b>Mohamad Makhzoum</b> , Cyber Security Specialist, Juniper Networks	<b>ManageEngine</b> <b>Decrypting the security mystery with SIEM</b> <b>Abishek Surendra Babu</b> , IT Security Specialist, ManageEngine	<b>SABSAcourses</b> <b>Refreshing your IT environment – a SABSA perspective</b> <b>Michael Hirschfeld</b> , Cyber Security Advisor, SABSAcourses	<b>Spire Solutions</b> <b>Is it time? The case for replacing your endpoint security stack</b> <b>Ashfak Pathan</b> , Senior Security Consultant, Spire Solutions	<b>Thales</b> <b>Embracing digital transformation and staying secure</b> <b>Hamid Qureshi</b> , Territory Sales Manager, Thales
13:30	Lunch and networking				
14:30	<b>Cybersecurity threats and solutions in the financial services sector: trends and latest technological developments</b> <b>Anshul Srivastav</b> , Chief Information and Digital Officer, Union Insurance <ul style="list-style-type: none"> <li>• What will be the biggest cybersecurity challenges faced by the financial services industry over the next year?</li> <li>• How have financial institutions used the latest technologies such as AI to address these challenges?</li> <li>• Looking to the future: how can developments such as AI and RegTech be used to aid the cybersecurity effort?</li> </ul>				
14:50	<b>Getting ready for the Cloud: changing cybersecurity requirements</b> <b>Nicolai Solling</b> , Chief Technology Officer, Help AG Middle East, and <b>Dr. Aleksandar Valjarevic</b> , Head of Solution Architecture, Help AG <ul style="list-style-type: none"> <li>• The Cloud delivers agility, speed and an OPEX-based cost model but Cloud services also fundamentally change cybersecurity requirements and processes</li> <li>• What you need to be aware of when it comes to Cloud security</li> <li>• Why you may need to re-think elements of your cyber and information security strategy when getting Cloud ready</li> </ul>				
15:10	<b>A brief walk through the cybercriminals' favourite tactic: social engineering, from its various types to a word of prevention</b> <b>Mahdi Naili</b> , Senior Systems Engineer, Fortinet Middle East, and <b>Kalle Björn</b> , Director, Systems Engineering – Middle East, Fortinet <ul style="list-style-type: none"> <li>• Psychological principles behind social engineering</li> <li>• Social engineering methods that fraudsters use</li> <li>• How to defend employees and your organisation and the importance of third-party testing</li> </ul>				
15:30	<b>EXECUTIVE PANEL DISCUSSION</b> <b>Cybersecurity threat intelligence and risk management</b> Chaired by: <b>Simon Moores</b> , Director, Zentelligence <b>Shafique Ibrahim</b> , Group Head of IT, Al Fardan Group <b>Ilham Ismail</b> , Head of IT, Hospitality Management Holdings <b>Scott Manson</b> , Leader of Middle East, McAfee, and <b>Vibin Shaju</b> , Director of Pre-Sales Southern Europe & MET, McAfee				
15:50	Networking and refreshments break				
16:10	<b>Case study: using Blockchain in the logistics industry</b> <b>Adam Lalani</b> , Group Head of IT, Tristar Transport <ul style="list-style-type: none"> <li>• What actually is Blockchain?</li> <li>• Using Blockchain for smart contracts and connected systems</li> <li>• Challenges to implementation and how these were overcome</li> </ul>				
16:30	<b>Just how important are the security basics in the fight against today's cybercrime?</b> <b>Brian Byagaba</b> , Head of Information Security, Commercial Bank International <ul style="list-style-type: none"> <li>• Understanding why having the basic cybersecurity principles in place is critical in the fight against cybercrime</li> <li>• Why anything extra is just a bonus</li> <li>• Elementary practices to protect our firms from cyber-attacks</li> </ul>				
16:50	<b>Increasing customer confidence in cybersecurity</b> <b>Hariprasad Chede</b> , Chief Information Security Officer, National Bank of Fujairah <ul style="list-style-type: none"> <li>• Arguably the biggest repercussions from a cyber-attack are the loss of customer confidence and brand reputation</li> <li>• Consumers are arguably becoming more conscious of what companies are doing with their data: what can we do to ensure consumer confidence?</li> <li>• Putting well-thought out initiatives into layman's terms</li> </ul>				
17:10	Closing remarks by <b>Simon Brady</b> , Managing Editor, AKJ Associates				
17:20	Conference close				

Education Seminars	
<p><b>Ground Labs</b></p> <p><b>Standards don't bother me – all I want is your data!</b></p> <p><b>John Cassidy</b>, Global Sales Leader, Ground Labs, and <b>Simon Davey</b>, Senior Business Development Executive, Ground Labs</p>	<p>How a business-as-usual approach to data security and performing sensitive data discovery can aid in achieving PCI and GDPR compliance.</p> <ul style="list-style-type: none"> <li>• Insights into how cybercriminals do not comply with global security standards, data theft is their only concern</li> <li>• Understanding the totality of your data helps in risk assessment for cybercrime</li> <li>• Data sprawl is one of the key challenges across corporate infrastructure as it presents a huge vulnerability to cybersecurity professionals</li> </ul>
<p><b>Juniper Networks</b></p> <p><b>The 101 on SDSN: why software-defined secure networks are changing the industry and what you need to know</b></p> <p><b>Mohamad Makhzoum</b>, Cyber Security Specialist, Juniper Networks</p>	<p>With the development of the digitalised industry, the threat landscape is changing. Organisations' networks are expanding, and so is their attack surface. There is a need for greater visibility, and new solutions that can provide that. Software-Defined Secure Network (SDSN) is quickly becoming many industry leaders' answer: allowing for a more efficient centrally managed, agile approach to security strategy. Software-Defined Secure Network (SDSN) provides end-to-end network visibility, allowing enterprises to secure their entire network, both physical and virtual, using threat detection and policy enforcement, an SDSN solution automates and centrally manages security in a multi-vendor environment. In this session, Fireware will be sharing actionable takeaways and unique insights into how to manage your SDSN journey.</p> <p><b>What attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• The changing landscape of network security and why end-to-end visibility is so important</li> <li>• The solution components and benefits: secure network, automated threat remediation, central management and multi-vendor ecosystem</li> <li>• Automated security for a virtual environment: how developments in technological innovation are changing our security needs and solutions</li> </ul>
<p><b>ManageEngine</b></p> <p><b>Decrypting the security mystery with SIEM</b></p> <p><b>Abishek Surendra Babu</b>, IT Security Specialist, ManageEngine</p>	<p>Most companies rely on the traditional security perimeter, which is proving no longer to be an effective cybersecurity control. They lack comprehensive, relevant and timely information in the wake of a breach. Also, the understanding of your business on these traditional security controls has always been lacking.</p> <p>In this session, Abishek will help you build a responsive security strategy and a logical security architecture using the SIEM solution at the heart of it, which in turn will help your IT and business run together.</p> <p><b>What attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• Why the traditional perimeter is no longer effective</li> <li>• Why is it important for your security application to understand your business?</li> <li>• How to integrate, incorporate and fully utilise the existing security controls and fill the gaps</li> <li>• What are the critical ingredients required for good SIEM deployment?</li> </ul>
<p><b>PGI</b></p> <p><b>Chasing the dream of the clean pipe: where are we today?</b></p> <p><b>Ahmed Husain</b>, CEO, Reload, on behalf of Protection Group International</p>	<p>If we look at the statement 'Plumbers save more lives than doctors', we realise what we have been doing wrong in battling cyber-attacks. Plumbers make sure the supply of water is as clean as possible for people to drink it, while doctors attempt to resolve symptoms once they are detected or reported. The cybersecurity industry started with the firewalls, IPS, and IDS devices being put on the pipe or internet line, and then because of the complexity of attacks we found ourselves acting as doctors and forgot our plumbing role. This talk will show the roadmap on how the industry is moving back towards the dream of a clean attack free internet pipe and what technologies exist or are coming next to make this dream come true.</p> <p><b>The talk will go over:</b></p> <ul style="list-style-type: none"> <li>• Limitations of technology and where the industry is heading towards</li> <li>• Practical training to alleviate the human factor</li> <li>• Effective policies and procedures towards safer clicks</li> <li>• Stitching it all together for cyber hygiene programme</li> <li>• Lessons learned from the GCC financial sector</li> </ul>

Education Seminars	
<p><b>Recorded Future</b></p> <p><b>The dark web’s deep threat intelligence secrets</b></p> <p><b>Nour Fateen,</b> Pre-Sales Consultant, Recorded Future</p>	<p>There has been much speculation (not to mention exaggeration) over recent years about the fabled dark web. We’ve heard how this shady underworld is the refuge of the cybercriminal elite. That this is their ‘Wolf’s Lair’, where they gather to plot the breaching of businesses and the hacking of celebrities amongst other activities.</p> <p><b>This presentation will feature:</b></p> <ul style="list-style-type: none"> <li>• A definition of the dark web and how it differs from other sources of intelligence</li> <li>• Real-world examples of threat actor activities in dark marketplaces</li> <li>• Methods for uncovering emerging threats using dark web sources</li> </ul>
<p><b>SABSAcourses</b></p> <p><b>Refreshing your IT environment – a SABSA perspective</b></p> <p><b>Michael Hirschfeld,</b> Cyber Security Advisor, SABSAcourses</p>	<p>In 2016, the Australian Department of Finance transitioned to an Electronic Work Environment (EWE). As Chief Information Officer and Chief Information Security Officer for the department, Michael led this transition navigating the technical and security related issues to deliver a modern flexible work platform. At the same time, he was responsible for the fit out and transition to a new, state of the art building.</p> <p>In this presentation, Michael will provide an overview of SABSA illustrating the strength of this security architecture framework through this unique case study. He will provide a high-level comparison of the architectural approaches taken in the physical (building) environment, the ICT environment and the information security environments to ensure the outcomes meet the needs of the business.</p> <p><b>What attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• The fundamentals of SABSA</li> <li>• How to develop a solid IT and cybersecurity strategy</li> <li>• How to align security requirements with business outcomes</li> <li>• How to drive transition and change in IT and security projects</li> <li>• High-level lessons learned through this project</li> </ul> <p>This case study highlights how the SABSA framework enhances the quality of outcomes and builds organisational confidence in the ICT and Information Security teams alike.</p>
<p><b>Spire Solutions</b></p> <p><b>Attack is the best form of defence!</b></p> <p><b>Siddhartha Murthinty,</b> Security Solutions Architect, Spire Solutions</p>	<p>It is imperative that organisations adopt attackers’ perspectives into their defences, strategies and offensive tactics. Join Spire’s Threat Exposure Management expert, Siddhartha Murthinty, in a session where he discusses insights into the attackers’ mindset, current vectors, and methodologies.</p> <p><b>Attendees will learn how to:</b></p> <ul style="list-style-type: none"> <li>• Uncover weaknesses in their defences, focus on the highest risks, and improve their security outcomes</li> <li>• Simulate real-world attacks to find their weak points before a malicious attacker does</li> <li>• Design Purple Team Assessment – test controls while under a simulated, targeted attack</li> <li>• Applying Defence in Depth to Detection &amp; Response</li> <li>• Shift Left with DevSecOps to embed security into testing</li> </ul>

<b>Education Seminars</b>	
<p><b>Spire Solutions</b></p> <p><b>Is it time? The case for replacing your endpoint security stack</b></p> <p><b>Ashfak Pathan,</b> Senior Security Consultant, Spire Solutions</p>	<p>Endpoint security has traditionally been reactive and focused on stopping file-based, malware-centric, and exploit-oriented attacks. As new threats appear, businesses invest in point products that address a specific objective such as a single attack vector (e.g., malware or application control) or compliance. As a result, enterprises have accumulated several solutions for AV, NGAV, IOC Search, exploit protection, and incident response tools.</p> <p>According to a recent Forrester survey, enterprises have on average more than seven endpoint tools to stop attacks. Each additional tool in the security stack makes it complex to operate, maintain, and costly.</p> <ul style="list-style-type: none"> <li>Choose an endpoint security solution that leverages a comprehensive attack model and covers the breadth and depth of techniques in the attacker’s tool kit</li> <li>Choose an endpoint tool that is intuitive and easy to operate without in-depth technical engineering knowledge</li> <li>Attackers take milliseconds to steal credentials or execute a ransomware attack. The speed of attacks requires protection that can stop these threats in milliseconds to be effective</li> </ul>
<p><b>Thales</b></p> <p><b>Embracing digital transformation and staying secure</b></p> <p><b>Hamid Qureshi,</b> Territory Sales Manager, Thales</p>	<p>Data breaches are the new normal. According to our 2018 Global Data Threat Report, 67% of enterprises have been breached, with that percentage rate growing every year. Regardless of the security measures and efforts put in place, organisations need to act as if a successful cyber-attack is not a question of ‘if’ but ‘when’. As organisations continue to embrace digital transformation, greater amounts of sensitive data is created, stored and transferred in digital form putting more data at risk. Also with the increase in cloud, mobile, and IoT devices, a whole new generation of attack surfaces are vulnerable to hackers. Just a few years ago the network perimeter were the four walls surrounding the corporate enterprise. With the emergence of these transformative technologies the perimeter has become dynamic and ever changing.</p> <p><b>What attendees will learn:</b></p> <ul style="list-style-type: none"> <li>How to navigate the world of digital transformation: embrace its advantages and mitigate its risks</li> <li>How has the increase in cloud, mobile, and IoT devices changed the threat landscape?</li> </ul>
<p><b>ThreatMetrix</b></p> <p><b>Digital identities, consumer identities and beyond...</b></p> <p><b>Michael Yeardley,</b> Senior Director, Product Strategy, ThreatMetrix</p>	<p>ThreatMetrix has a long, established and proven development roadmap that has ensured its customers are tackle the evolving challenges from the digital economy. With the acquisition by Lexis Nexis, it now has the ability to leverage digital, physical and consumer identities, and extend the way in which it can address both the known, and unknown challenges facing companies across the globe.</p> <p>Leveraging its unique position, developing new and extended customer use cases, ThreatMetrix continues to empower its customers and benefit from its ability to leverage the intelligence inherent within a dynamic, global digital identity network – and meet challenges head on.</p> <p><b>What attendees will learn:</b></p> <ul style="list-style-type: none"> <li>A review of the latest 2018 cybercrime trends, based on actual attacks detected by the ThreatMetrix Digital Identity Network.</li> <li>The benefits of sharing – digital and consumer identities</li> <li>What’s next – how ThreatMetrix continues to evolve and tackle the challenges of a global digital economy head on</li> <li>How to achieve data security and compliance with an Encrypt Everything Strategy</li> </ul>