

Post event report



The 10th e-Crime & Cybersecurity Congress in Dubai

20th March 2018 | Dubai, UAE

Principal Sponsor



Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



“Yesterday’s congress and its resultant presentations and networking activities was most definitely a great deal of help to me in terms of flourishing my knowledge base and getting a chance to have a complete view on the IT security industry; zero-doubt about the fact that it was one of the most profitable and fruitful events I have ever attended.”

Director, Customer Operations, D-Smart

“I take this opportunity to thank you and your team for organising a wonderful event ‘10th e-Crime & Cybersecurity Congress’. You all did an absolutely blinding job of organising this event – in particular with regard to the venue, topics and speakers. It was a really enjoyable learning symposium. There was a good balance of presentations. I appreciate the sessions led by industry experts. And how nice it was of them to make themselves available for the full day to meet and answer local and international community questions. Once again, thank you for the invitation to attend the 10th e-Crime & Cybersecurity Congress, this was a delightful experience.”

CCO, Orient Exchange Co. (L.L.C.)

“As always, the event was very well organised. The organising team were excellent. No doubts in it. I felt the presentations were quite simple and matured. Education sessions were excellent and this time I came to know about the presence of some new vendors and their solutions. This congress has always been a value addition to my knowledge.”

Information Security Manager, RSA Insurance Group

Inside this report:

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



Speakers

- Chris Adam, Solutions Engineer, **Cloudflare**
- Sumit Agarwal, Co-founder and COO, **Shape Security**
- Laith Alkhouri, Co-founder & Director of Advanced Solutions, **Flashpoint**
- Rizwan Arain, Chief Information Security Officer, **Habib Bank AG Zurich**
- Mohammad Ashour, Head of Audit and Compliance Department, **Arab Bank for Investment and Foreign Trade**
- Oliver Bendig, CEO, **Matrix42**
- Simon Brady, Managing Editor, **AKJ Associates**
- Serhat Candan, VP Product and Strategy, **SECURENT**
- Joseph Carson, Chief Security Scientist, **Thycotic**
- Ganesh Chellappa, Manager – Support and Client Services, **ManageEngine**
- Chris Coleman, CEO, **LookingGlass Cyber Solutions**
- Jay Coley, Senior Director – Security Strategy and Planning EMEA, **AkamaiTechnologies**
- Nour Fateen, Technical Consultant, **Recorded Future**
- Ankush Johar, Director, Infosec Ventures, on behalf of **Spire Solutions**
- Jonathan Martin, EMEA Operations Director, **Anomali**
- Simon Moores, Director, **Zentelligence (Research) Ltd**
- Mike Murray, VP of Security Intelligence, **Lookout**
- Amanda Oon, Senior Conference Producer/Deputy Editor, **AKJ Associates**
- Matthew Platten, Anti-Fraud Solutions Consultant EMEA, **Easy Solutions**
- Hamid Qureshi, Territory Sales Manager, Middle East, **Thales eSecurity**
- K.S.Ramakrishnan, Chief Risk Officer, **RAK Bank**
- Tilak Ratnayake, Group IT Infrastructure Manager, **GAC Group**
- Sameh Sabry, VP – Engineering, **Spire Solutions**
- Abbas Sabuwala, Head of IT Services & Information Security, **UASC**
- Barry Scott, CTO, EMEA, **Centrify**
- Vibin Shaju, Regional PreSales Manager, Middle East & Turkey (MET), **McAfee**
- Neil Thacker, CISO, **Netskope**
- Ramesh Veera, Executive Director, Risk & Compliance, **National Bonds Corporation**
- Sivakumar Venkatraman, Chief Information Officer, **Dubai First**
- Robert Walker, Managing Director, **AKJ Associates**

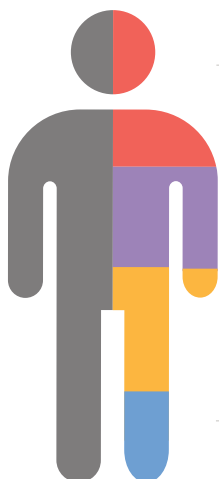
Key themes

Securing email and social media

Employee awareness and engagement

Cyber-threats and responses in the financial sector

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

Agenda					
08:00	Breakfast networking and registration				
08:50	Opening remarks				
09:00	Cyber-risk strategy – adopting a risk-based approach to effective cybersecurity				
	<p>Rizwan Arain, Chief Information Security Officer, Habib Bank AG Zurich</p> <ul style="list-style-type: none"> • Different methodologies that organisations use to meet cybersecurity requirements • Examples from the financial services: How banks and other organisations focus their security endeavours on meeting regulatory requirements • Why organisations need to deploy a risk-based approach to deal with cybersecurity that plays out a comprehensive evaluation of the threats 				
09:20	Why security leaders should be aware of terrorist threats				
	<p>Laith Alkhouri, Co-founder & Director of Advanced Solutions, Flashpoint</p> <ul style="list-style-type: none"> • Where does a great deal of threatening activity on the internet emerge from? • What is the Deep and Dark Web and how can having Dark Web visibility help protect your organisation? • How can we look at threats from a proactive standpoint and why is incident response not enough? • How can physical and cyber teams work together to mitigate the hybrid risk posed by violent non-nation state actors (VNSA)? 				
09:40	Do you think IOAMA is secure?				
	Sumit Agarwal , Co-founder and COO, Shape Security				
10:00	A brief history of tomorrow				
	<p>Simon Moores, Director, Zentelligence (Research) Ltd</p> <ul style="list-style-type: none"> • A matter of scale. What we learned from 2017 • Intelligence at the edge: A security revolution is required • Bitcoin and the blockchain. 'A computationally burdensome way to hate the Government?' • AI – a technology steadily reaching maturity in security and information governance • Machine learning goes mobile 				
10:20	Education Seminars Session 1				
	<p>Cloudflare Mitigating large scale DDoS Chris Adam, Solutions Engineer, Cloudflare</p>	<p>Easy Solutions Breaking the fraud cycle Matthew Platten, Anti-Fraud Solutions Consultant EMEA, Easy Solutions</p>	<p>Matrix42 Automated endpoint security in a VUCA world Oliver Bendig, CEO, Matrix42</p>	<p>Spire Solutions Is your endpoint security product protecting you from targeted attacks? Sameh Sabry, VP – Engineering, Spire Solutions</p>	<p>Thales eSecurity In a world of digital transformation, achieve data security and compliance with an Encrypt Everything Strategy Hamid Qureshi, Territory Sales Manager, Middle East, Thales eSecurity</p>
11:00	Refreshments and networking break				
11:30	When CROs get cyber savvy				
	<p>K.S.Ramakrishnan, Chief Risk Officer, RAK Bank</p> <ul style="list-style-type: none"> • Why cybersecurity is the first thing on your CRO's mind • Why organisations need a clear cyber-risk modelling strategy • Importance of cyber-risk management in financial services • Practical tips to deal and gain management support to enhance control environment 				
11:50	Protecting innovation in a perimeterless world				
	<p>Neil Thacker, CISO, Netskope</p> <ul style="list-style-type: none"> • Threat: Review the latest threats targeting organisations including the use of backdoors in cloud-based malware • Governance: Understand how to protect intellectual property and associated data during the IP lifecycle • Resilience: Steps to take to automate incident response and to uncover both common and future blind spots 				
12:10	The Dark Web's deep threat intelligence secrets				
	<p>Nour Fateen, Technical Consultant, Recorded Future</p> <ul style="list-style-type: none"> • A definition of the Dark Web and how it differs from other sources of intelligence • Real-world examples of threat actor activities in dark marketplaces • Methods for uncovering emerging threats using Dark Web sources 				
12:30	Zero Trust Security – Never Trust, Always Verify				
	<p>Barry Scott, CTO, EMEA, Centrifly</p> <p>Organisations spent a combined \$170 billion on cybersecurity in 2016 and 2017. During the same period, 66% of organisations experienced an average of five or more data breaches. A larger security budget simply won't solve the cybersecurity problem. An entirely new approach is required – Zero Trust Security.</p> <p>The benefits of Zero Trust Security are crucially important in this climate of ever increasing number and scope of security breaches. Zero Trust Security:</p> <ul style="list-style-type: none"> • Covers the broadest range of attack surfaces, ranging from users, endpoints, and networks to resources • Enables organisations to increase business agility through the secure adoption of cloud and mobile solutions • Provides a framework to properly manage the risk of exposing sensitive apps and infrastructure to business partners • Creates satisfied, productive users by ensuring the proper controls are in place to address appropriate levels of risk without requiring a heavy-handed, maximum-control approach regardless of the risk posed 				

Agenda				
12:50	Education Seminars Session 2			
	Anomali Log data? Make it relevant, fight adversaries and win Jonathan Martin, EMEA Operations Director, Anomali	ManageEngine Keys to the Kingdom – Strategies for managing privileged identify Ganesh Chellappa, Manager – Support and Client Services, ManageEngine	SECURENT What is the new normal in cybersecurity? How to prepare for fifth generation of cyber-attacks Serhat Candan, VP Product and Strategy, SECURENT	Spire Solutions Solving the two BIGGEST challenges in cybersecurity. Learn from top CISOs’ case studies Ankush Johar, Director, Infosec Ventures, on behalf of Spire Solutions
13:30	Lunch and networking			
14:30	EXECUTIVE PANEL DISCUSSION			
	When security gets mission critical: Protecting core business assets and CNI			
Tilak Ratnayake, Group IT Infrastructure Manager, GAC Group Mohammad Ashour, Head of Audit and Compliance Department, Arab Bank for Investment and Foreign Trade Abbas Sabuwala, Head of IT Services & Information Security, UASC Sivakumar Venkatraman, Chief Information Officer, Dubai First Vibin Shaju, Regional PreSales Manager, Middle East & Turkey (MET), McAfee				
14:50	Protecting organisations against the full spectrum of mobile risk			
Mike Murray, VP of Security Intelligence, Lookout <ul style="list-style-type: none"> • What are the full spectrum of mobile risks? • How everyday employee behaviours can jeopardise your data, systems, and compliance policies • Mobile security best practices • Evolving beyond mobile device management • The in’s and out’s of threat intelligence – including Dark Caracal, the first globally active mobile APT 				
15:10	How to future proof your security strategy			
Jay Coley, Senior Director – Security Strategy and Planning EMEA, Akamai Technologies <ul style="list-style-type: none"> • Having a DDoS mitigation plan in place can make the difference between organisation-wide chaos and an orderly and timely DDoS response. What steps can you take to prepare? • Mirai and recent banking attacks stress your security perimeters have to evolve faster than your attackers. How do you stay ahead in the constantly changing threat landscape? • Performing analysis to prioritise what needs protecting is key. Are you ready for the next attack? 				
15:30	Reversing the economics of cybercrime			
Chris Coleman, CEO, LookingGlass Cyber Solutions <ul style="list-style-type: none"> • Share an overview of the current GCC cybersecurity landscape, highlighting the financial and the oil/gas verticals • Discuss the economics of cybercrime with a focus on the criminal’s return on investment (ROI) • Explore how businesses can change the cybercriminal’s ROI to diminish their likelihood of being targeted 				
15:50	An integrated and pragmatic approach to cyber-risk management			
Ramesh Veera, Executive Director, Risk & Compliance, National Bonds Corporation <ul style="list-style-type: none"> • Importance of a comprehensive cyber-risk strategy for an organisation • Promote common understanding of cyber-risk across the organisation • Balancing cyber-risk with the growing trends of digital innovation • Improving risk culture towards better management of cyber-risk 				
16:10	Networking and refreshments			
16:30	The anatomy of a privileged account hack: Inside the MIND of a hacker			
Joseph Carson, Chief Security Scientist, Thycotic <ul style="list-style-type: none"> • This session describes the anatomy of a privileged account hack • We will show how cybercriminals target their victims • What you can do to reduce your risk and prevent abuse of your critical information asset 				
16:50	Cybersecurity in the UAE revealed			
Simon Brady, Managing Editor, AKJ Associates; and Amanda Oon, Senior Conference Producer/Deputy Editor, AKJ Associates <ul style="list-style-type: none"> • Navigating the vendor ecosystem: What CISOs really feel about their suppliers • What are your top three priorities in a cybersecurity solutions provider? • Identifying your unique business risk and the right partners to help you mitigate it • Compare and contrast: The UAE and European cybersecurity market. And how you’ve rated them 				
17:10	End of conference and closing remarks by Robert Walker, Managing Director, AKJ Associates			

Education Seminars	
<p>Anomali</p> <p>Log data? Make it relevant, fight adversaries and win</p> <p>Jonathan Martin, EMEA Operations Director, Anomali</p>	<p>Most organisations diligently generate billions of logs per day, whether in a SIEM or a log management tool, via syslog or via flow data. However, they are increasingly finding it more and more problematic to cope with the issues of detecting breaches using that log data. This is because current tools were never designed to cope with the huge volume of Cyber Threat Intelligence (CTI) being created and disseminated – put simply, we have to adopt a new approach to solving the problem of breach detection and analysis using the latest threat intelligence tools.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • The differences between threat data, threat intelligence and relevant, risk-based threats • How to integrate CTI into their existing security environment to generate greater return of investment • The extra components required to move from an existing first generation Security Operations Centre (SOC) to the latest SOC 2.0. • What customers need to build a threat platform for business risk
<p>Cloudflare</p> <p>Mitigating large scale DDoS</p> <p>Chris Adam, Solutions Engineer, Cloudflare</p>	<p>Distributed denial of service (DDoS) attacks are on the rise. In 2016, the Mirai botnet caused a large portion of the internet to become unavailable when it attacked a large DNS provider. That attack consumed over 1 terabit per second of bandwidth. In 2018, the internet has already witnessed attacks measuring up to 1.7 Tb/s. In this educational seminar, Chris Adam will discuss how the DDoS threat landscape is changing and what you can do to protect your business from these common attacks.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • What is a DDoS? • Am I vulnerable? • How can I defend my business from these attacks?
<p>Easy Solutions</p> <p>Breaking the fraud cycle</p> <p>Matthew Platten, Anti-Fraud Solutions Consultant, Easy Solutions</p>	<p>Cases of electronic fraud are costing organisations and consumers more than \$16 billion globally. From lack of visibility to weak password hygiene, the contributed factors are far too many. Industry experts agree that while there is no silver bullet to combat electronic fraud yet, a multi-layered approach is what has proven most effective.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • What <i>really</i> comprises a multi-layered approach • An overview of a typical attack method • Real-life cases of the most sophisticated internet attacks • Fraud trends to expect in 2018 • An actionable plan on breaking the fraud cycle
<p>ManageEngine</p> <p>Keys to the Kingdom – Strategies for managing privileged identify</p> <p>Ganesh Chellappa, Manager – Support and Client Services, ManageEngine</p>	<p>What attendees will learn:</p> <ul style="list-style-type: none"> • The seven domains of a typical IT infrastructure • Types of authentication: Who is the winner? • Privileged access: What is it and who needs it? • Future and best practices
<p>Matrix42</p> <p>Automated endpoint security in a VUCA world</p> <p>Oliver Bendig, CEO, Matrix42</p>	<p>Across all industries, we now live in a VUCA world. It is mobile, intelligent, connected, and it is under attack. Digital transformation is evolving faster than security know how. What is our natural response to these new threats? In this presentation, we will explore the VUCA world, and analyse cybersecurity as a business enabler and innovator.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • VUCA is the new normal: Introduction to a VUCA world • Why is automated endpoint security the only solution? • How to deal with digital transformation and the advancement of machine learning

Education Seminars

SECURRENT

What is the new normal in cybersecurity? How to prepare for fifth generation of cyber-attacks

Serhat Candan, VP Product and Strategy, SECURRENT

According to World Economic Forum’s annual global risk report in 2018, cybersecurity has become the third largest threat after extreme weather events and natural disasters. 2017 was a global wake-up call to get serious about addressing the cyber-threat landscape. What would once have been considered large-scale attacks are now normal.

Unprecedented levels of cyber-attacks played out as large-scale, multi-vector mega attacks that inflicted major damage on business and reputation. Hackers are exploiting the fact that most organisations rely on older generations of security. As the sophistication and scale of attacks has grown, previous generations of security, which merely detect, are no longer effective. To succeed in business now, we must evolve to a new generation of cybersecurity: Gen V.

What attendees will learn:

- How to scale up the security controls in the rapid digital transformation of business (automation and orchestration of security)
- How to enable preemptive protection across all platforms including cloud and mobile (the new weakest link of the chain: mobile devices)
- How to enable real-time threat prevention across the entire enterprise (single security architecture and threat intelligence)
- How anomaly detection and machine learning are helping us to fight against unknown attacks
- Bonus: TL;DR What are prediction reports telling about 2018?

Spire Solutions

Solving the two BIGGEST challenges in cybersecurity. Learn from top CISOs’ case studies

Ankush Johar, Director, Infosec Ventures, on behalf of Spire Solutions

Email is the #1 attack vector, and humans are the weakest link in cybersecurity! There is no point in investing millions, when all it takes is under \$5 to break the security you create with the millions. See the speaker take on a live & open challenge from anyone in the audience to demonstrate the threat. This will be followed by an explanation on how this threat can be mitigated, and also why the US Department of Homeland Security has made this mitigation mandatory under a binding directive in October 2017. Ankush Johar is a technocrat and an investor in cybersecurity innovators that solve BIG problems, with notable investments in BugsBounty.com, EmailAuth, HumanFirewall, InfoSecSSG among others.

What attendees will learn:

- How to mitigate the two biggest risks in cybersecurity? Learn from the masters.

#EMAILAUTHENTICATION

- What are the three attack types in email and how to mitigate against them (in under three mins). Every attendee will receive a free kit
- If a hacker spoofs you to send email to third parties (external server to external server), see how you can still get to know, and more importantly block it from being delivered. The kit contains information on how to receive this threat intelligence
- How to use EmailRemediator.com techniques to remediate an email attack in under three minutes. Live show. Audience will send an attack email, and speaker will remediate it from across over 120,000+ employees in under three minutes

#HUMANFIREWALL

- CISOs are ALWAYS at the receiving end! See how to reverse that trend once and for all. Gain the power
- How the best CISOs are using the six facets of ‘human psychology’ + using ‘employee powered’ cybersecurity techniques to transform humans into the strongest link in cybersecurity
- With over 10,000+ types of common attacks, it is impossible to keep cyber awareness programmes up to date. See how this financial institution deployed their HumanFirewall
- How to enable employees such that one person is empowered to save the entire organisation. Gamify-Gamify-Gamify!
- What you can measure, you can manage. Learn about how the masters are measuring their ‘Human Information Security Preparedness™’ and how they are reporting it to their board. There is finally a metric for it now!

Education Seminars	
<p>Spire Solutions</p> <p>Is your endpoint security product protecting you from targeted attacks?</p> <p>Sameh Sabry, VP – Engineering, Spire Solutions</p>	<p>Targeted cyber-attacks are having a profound effect on enterprises. These attacks are 100% successful because they ‘outperform’ security programmes. A fundamental problem of most programmes is that they do not have a robust attacker model that accounts for the attacker behaviour. Organisations need defences against the full scope of techniques to rapidly detect and remediate before damage and loss.</p> <p>Join Spire’s Associate Vice President, Sameh Sabry, in a session where he discusses how organisations can build a robust security programme addressing their people, process, and technology to stop targeted attacks.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • What are ‘targeted attacks’ and why are they ‘100% successful’? • Current security programmes and what they lack • Why endgame is the only endpoint security solution that can stop targeted attacks before damage and loss • Endgame’s Zero Breach Tolerance model and how effective it is against targeted attacks
<p>Thales eSecurity</p> <p>In a world of digital transformation, achieve data security and compliance with an Encrypt Everything Strategy</p> <p>Hamid Qureshi, Territory Sales Manager, Middle East, Thales eSecurity</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>What attendees will learn:</p> <ul style="list-style-type: none"> • How to navigate the world of digital transformation: embrace its advantages and mitigate its risks • How has the increase in cloud, mobile, and IoT devices changed the threat landscape? • How to achieve data security and compliance with an Encrypt Everything Strategy