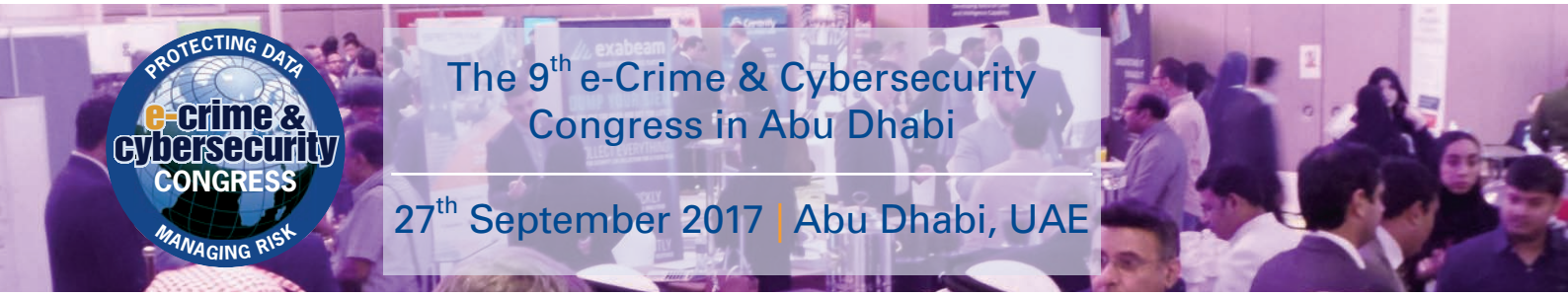
Post event report



The 9th e-Crime & Cybersecurity Congress in Abu Dhabi

27th September 2017 | Abu Dhabi, UAE

Principal Sponsor

GBM

Strategic sponsors

Centrify – THE BREACH STOPS HERE

DARKTRACE

FIREMON

FORTINET

IBM

PHISHME

thycotic

wombat security technologies

Education Seminar Sponsors

Flowmon – Driving Network Visibility

ManageEngine

PGI

Recorded Future

SABSA COURSES.COM

Networking Sponsors

ANOMALI

Arcon

Check Point SOFTWARE TECHNOLOGIES LTD.

CLOUDFLARE

CYBERGATE

exabeam

Green Method

Network Security Virtualization TNCT

VASC

Consultancy Sponsor

wsp

"This is the second time that I have attended the e-Crime & Cybersecurity summit in Abu Dhabi and it turns out to be better each year. This year we had speakers who were very much focused on current digital threats, How to overcome them and also preventive methods. I managed to network with a lot of information security individuals and exchanged, as well as gained, knowledge. The event was organised very well, keeping up with the time and contents. I look forward to the next one."

Assistant Manager, Forensic Technology & Discovery Services – Middle East & North Africa, EY Middle East & North Africa

"Thank you one again for the invitation and excellent organisation of this valuable event. This is my third time attending e-Crime & Cybersecurity Abu Dhabi and I must say that every time I'm surprised by the quality and diversity this event brings to the cybersecurity audience. The networking, panels and presentations have been very interesting and I will end up in future engagements with some of the presented vendors on their solutions. So thank you and I look forward to next year's event."

ICT Technical Security Specialist, ICT Technical Security Services

"Attending e-Crime & Cybersecurity Abu Dhabi was a great pleasure; I was surprised with the excellent arrangement and the careful selection of security topics that are very much relevant to what we need to know about and work on to improve our security. Many thanks to all your team and I will be looking forward to attending your event every year."

Infrastructure and Security Manager, Emirates National Oil Company Limited (ENOC) LLC

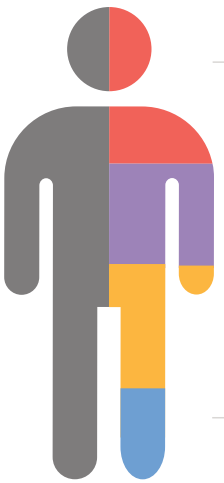
Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

Key themes

- Smart cities: More dangerous, more costly than analog?
- Consequences of the cloud
- Proving the business value of security
- Payments innovation and cyber risk
- Securing the banking industry
- Securing staff and protecting employees
- The foundations of cyber resilience

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

Ashraf Abdelazim, MEA Region Leader; and Craig Roberts, EMEA Sales Engineer, IBM Resilient

Ranuka Angammana, Director of IT, Rotana Hotels Management Corporation

Kuldeep Bhatnagar, CISO, Environment Agency, Abu Dhabi Government

Kalle Björn, Director, Systems Engineering – Middle East, Fortinet

Joseph Carson, Chief Security Scientist, Thycotic

Elizabeth De Freitas, Regional Manager, Darktrace

Kevin Flanagan, VP Sales Engineering, PhishMe

Bruno Fonseca, CISO, AXA Insurance Gulf

Rakesh Gohil, Senior Director – ICT, Seddiqi Holding

Kashif Khan, Head of Information Security Risk, Abu Dhabi National Insurance Company (ADNIC)

Suraj Khetani, Regional Associate Security Consultant, Gulf Business Machines

Dawid Kowalski, Technical Director – EMEA, FireMon

Charles Lewis, Senior Consultant, SABSAcourses

Marek Machálek, Area Manager MEA, Flowmon Networks

Sebastian Madden, Chief Corporate Development Officer, PGI

Steve Mair, Senior Cyber Security Consultant, PGI

Simon Moores, CEO, Zentelligence

André Mouradian, EMEA Marketing Manager, Wombat Security Technologies

Hani Nofal, Vice President, Gulf Business Machines

Chris Pace, Technology Advocate, Recorded Future

Sharique Rizvi, Senior Forensic Investigator and Head of IT Security, Supreme Group

Akhtar Rasool, Lead Regional Security Consultant, Gulf Business Machines

Carl Salji, Technical Director MENA, Darktrace

Barry Scott, CTO, EMEA, Centrify

Rehan Siddiki, General Manager, Information Security, VFS TasHeel

Siddharth Sharathkumar, IT Security Specialist, ManageEngine

Agenda

08:00 Registration

08:50 Conference welcome by **Robert Walker,** Managing Director, AKJ Associates/**Simon Brady,** Managing Editor, AKJ Associates

09:00 **Private public collaboration: Staying smart about Smart**

Kuldeep Bhatnagar, CISO, Environment Agency, Abu Dhabi Government
- The role of the government/public sector in the development of Smart cities
- Securing critical national infrastructure and the relationship between public and private industry
- Case studies from private to public industry

09:20 **The evolution of GCC enterprises: Are they ready for the next generation?**

Hani Nofal, Vice President, Gulf Business Machines
- In-depth research scanning of three generations (Gen X, Gen Y, Gen Z) views on security and mobility
- Misperception and expectation on security between Gen X and Gen Y
- Recommendations on embracing the next generation expectations

09:40 **Back to basics: Why we need to re-evaluate cyber, business continuity, and their relationship**

Bruno Fonseca, CISO, AXA Insurance Gulf
- The need for incident response that aligns cybersecurity and business security
- The effect of high-profile global attacks like Wannacry on how stakeholders and business leaders value cyber
- Budgeting and how cyber value and metrics is more than just getting budget

10:00 **70 million responses can't be wrong**

André Mouradian, EMEA Marketing Manager, Wombat Security Technologies
- Gain key insights into end user cybersecurity knowledge
- Share results of our 2017 Beyond the Phish Report, analysing the aggregate data of 70 million responses to security questions and training challenges across 11 different topics
- Learn in which topics end users are the strongest and the weakest so that you can determine how to plan or improve your security awareness and training programme
- Understand knowledge in various industries and how they differ so that you can have a benchmark against which to compare your end users' knowledge
- We'll provide guidance about how to use this information to strengthen your carbon-based defences and reduce the risk of successful cyber attacks

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

Flowmon Networks	Gulf Business Machines	PGI	Recorded Future
Network behaviour analysis – how to fight against modern cybersecurity threats **Marek Machálek,** Area Manager MEA, Flowmon Networks	**The art of deceiving humans 'Social Engineering'** **Suraj Khetani,** Regional Associate Security Consultant, Gulf Business Machines	**Choosing your information security management systems – a framework for decision making** **Steve Mair,** Senior Cyber Security Consultant, PGI; and **Sebastian Madden,** Chief Corporate Development Officer, PGI	**Best practices for applying threat intelligence** **Chris Pace,** Technology Advocate, Recorded Future

11:00 Networking break and refreshments

11:30 **The true value of cybersecurity: A practical guide to crisis management and board engagement**

Rakesh Gohil, Senior Director – ICT, Seddiqi Holding
- Why security is so much more than an operations/infrastructure role. Every department needs to have a plan
- Crisis management and prevention. Practical tips
- Getting the board on board: Communicating the brand reputation, financial risks, share price drop of a breach in business terms

11:50 **Is your security management solution keeping up?**

Dawid Kowalski, Technical Director – EMEA, FireMon
- Managing the complexity of next generation security infrastructures
- Achieving security agility, reducing security risk and responding to threats faster

12.10 **Email security: Why is it still a problem?**

Kevin Flanagan, VP Sales Engineering, PhishMe
- With the majority of recent breaches starting with a phishing attack, phishing continues to be the number 1 malware delivery mechanism targeting organisations today
- Despite the massive investment in layered 'next generation' technology deployments to stop attackers, security professionals continue to struggle with preventing malicious email from getting into a user's inbox and stopping users from clicking on links or attachments when delivered
- This session will discuss trends and statistics on attacks and end user susceptibility collected from phishing campaigns across thousands of global organisations across 21 industries
- It will then discuss best practices for increased visibility, executive awareness, and end user conditioning that will minimise risk through focused phishing detection and incident response

Agenda

12.30 **The Enterprise Immune System: Using machine learning for next-generation cyber defence**

Elizabeth De Freitas, Regional Manager, Darktrace; and **Carl Salji,** Technical Director MENA, Darktrace
- How new machine learning and mathematics are automating advanced cyber defence
- Why 100% network visibility allows you to detect threats as they happen, or before they happen
- How smart prioritisation and visualisation of threats allows for better resource allocation and lower risk
- Real-world examples of unknown threats detected by 'immune system' technology

12:50 **Education Seminars | Session 2**

Gulf Business Machines	ManageEngine	PGI	SABSAcourses	Thycotic
Security architecture transformation: How to simplify security architecture design? **Akhtar Rasool,** Lead Regional Security Consultant, Gulf Business Machines	**Building an enterprise security strategy by leveraging SIEM** **Siddharth Sharathkumar,** IT Security Specialist, ManageEngine	**Bridging the cyber skills gap – practical steps to building a roadmap** **Steve Mair,** Senior Cyber Security Consultant, PGI; and **Sebastian Madden,** Chief Corporate Development Officer, PGI	**Architecting a multi-tiered control strategy** **Charles Lewis,** Senior Consultant, SABSAcourses	**The evolving perimeter – where are the new boundaries?** **Joseph Carson,** Chief Security Scientist, Thycotic

13:30 Lunch

14:30 **PANEL DISCUSSION** **Securing critical assets**

Ranuka Angammana, Director of IT, Rotana Hotels Management Corporation
Kashif Khan, Head of Information Security Risk, Abu Dhabi National Insurance Company (ADNIC)
Sharique Rizvi, Senior Forensic Investigator and Head of IT Security, Supreme Group
Joseph Carson, Chief Security Scientist, Thycotic

14:50 **IAM done right**

Barry Scott, CTO, EMEA, Centrify
Are you moving your applications to the cloud or have a cloud first strategy? Most recent data breaches have focused on user accounts and privileged access to sensitive resources, both in the data centre and in the cloud. While you are migrating to cloud platforms, now is the time to re-think security. In this session, we will explore proven best practices for protecting:
- Identities
- Privileged access
- Across data centres and cloud-based services

15:10 **And the beat goes on…the evolving threat landscape versus advanced threat protection**

Kalle Björn, Director, Systems Engineering – Middle East, Fortinet
- How has the Advanced Threat Protection evolved in recent years?
- What can be done to share threat information openly between different systems?
- How to integrate the ATP solution with rest of the network?

15:30 **The role of orchestration and automation in incident response maturity**

Ashraf Abdelazim, MEA Region Leader; and **Craig Roberts,** EMEA Sales Engineer, IBM Resilient
- What's the difference between automation and orchestration in incident response and the current industry landscape for IR?
- How to build maturity and capability in your environment for incident response
- Use case: Building a modern SOC and proactive IR

15:50 Networking break and refreshments

16:10 **The actionable security strategy: How to implement a cybersecurity culture with measurable results**

Rehan Siddiki, General Manager, Information Security, VFS TasHeel
- Everyone talks about culture, but how do you make it measurable?
- The tangible benefits of security awareness
- Case studies towards maturity and board level access

16:30 **Steps to cybersecurity success**

Simon Moores, CEO, Zentelligence
- Is there a blueprint for enterprise security management?
- Do we need to finally accept that business may never be fully equipped with the tools to manage cyber risks with the same level of confidence that they manage other risks?
- The new field of cyber risk
- Is AI being dramatically oversold?

16:50 Closing remarks

17:00 Close of conference

Education Seminars

Flowmon Networks

Network behaviour analysis – how to fight against modern cybersecurity threats

Marek Machálek, Area Manager MEA, Flowmon Networks

The rise of unknown malware compromising internal systems, devastating DDoS attacks, APTs and threats bypassing traditional security have changed the IT security landscape. Building perimeter walls and relying on signature-based solutions is not enough anymore. Only a detailed awareness of network behaviour and a proactive fight against cyber threats can give control over the IT environment back to administrators.

Most companies rely on legacy IT systems, consisting of perimeter security and endpoint protection. However, they dismiss the significant infrastructure located between these two areas. In the world where threats have more opportunities than ever to bypass traditional solutions and sneak in, where 70% of attacks come from an internal network, this approach is not enough anymore. How do you secure your systems and data from sophisticated, ever-changing threats that are undetectable by traditional solutions?

The answer to this challenge recommended by respected authorities such as Gartner is a proactive detection and mitigation of network anomalies and undesirable behaviour. This is provided by network monitoring solutions equipped with powerful artificial intelligence called Network Behaviour Anomaly Detection (NBAD). NBAD solutions permanently observe network traffic, analysing communication to seek anomalies and reveal suspicious behaviour. This enables a response to yet unknown security threats undetectable by other technologies.

What attendees will learn:

- How to have a detailed awareness of what is happening in the network
- How to utilise network traffic statistics exported by routers/switches or network probes to detect malicious behaviour
- How to complete the security circle by a complementary solution for detecting advanced threats bypassing traditional solutions, e.g. targeted attacks, botnets, unknown malware, insider threats, data leakage, etc.
- How to streamline network operations by the automatic detection of anomalies and operational issues

Gulf Business Machines

The art of deceiving humans 'Social Engineering'

Suraj Khetani, Regional Associate Security Consultant, Gulf Business Machines

With much invested on R&D in the hacking industry, hackers are becoming more innovative than ever in compromising organisations, whether ransomware, phishing or social engineering, etc.…

Are you thinking how to prevent your people from being the next hacked target? Well, it is not that easy!

With the tendency of people exposing their life on the internet and the lack of awareness on prevention tactics, hackers are gathering information to hit their next target and so many people still often tend to be tricked into clicking links and running enticing looking documents that end up being malicious and usually bypass anti-virus protection mechanisms.

In the speaker's opinion, social engineers are mastering their skills like pretexting, elicitation, information gathering skills, interrogation skills, influence skills and manipulation skills using Open Source Intelligence (OSNIT) but you are still protected if you have the key to mitigate them. Join us in an interesting social engineering session followed with live hacking scenarios.

What attendees will learn:

- Looking to be a Social Engineer, get ready to be introduced to the pretext skill
- How can OSNIT get you hacked?
- How can you protect yourself against social engineering attacks?

Education Seminars

Gulf Business Machines

Security architecture transformation: How to simplify security architecture design?

Akhtar Rasool, Lead Regional Security Consultant, Gulf Business Machines

As millennials in enterprises are marketing the digital culture, and the number of people, things and devices that are intelligently connected are dramatically increasing, hackers have never been busier! But the question is, can enterprises be secure and agile at the same time? Can your business be secured at all levels and still be within budget?

In this session, GBM Lead Security Consultant will take you on a holistic journey to develop the next-generation security architecture that meets your growing demands.

What attendees will learn:

- What does holistic and integrated security architecture design really mean?
- The five fundamentals for secured next-generation enterprises
- Moving from high risk and low agility to a state of low risk and high agility (Win-Win)

ManageEngine

Building an enterprise security strategy by leveraging SIEM

Siddharth Sharathkumar, IT Security Specialist, ManageEngine

One of the biggest roadblocks security professionals face is the lack of comprehensive, relevant and timely information in the wake of a breach.

In this session, Siddharth will help you build a responsive security operations centre (SOC) by formulating a cybersecurity strategy with a SIEM solution at the heart of it.

What attendees will learn:

- How to assess cyber threats, outline security strategy, and come up with best practices in your security operations centre
- Why security auditing and setting up optimal auditing policies is important
- Learn to execute your enterprise security strategy by deploying a SIEM solution

PGI

Choosing your information security management systems – a framework for decision making

Steve Mair, Senior Cyber Security Consultant, PGI; and **Sebastian Madden,** Chief Corporate Development Officer, PGI

There are several different security management systems in use globally, but how do you know which is the right one for your business?

In this session, we'll look at some of the most common security models and security management systems (such as ISO 27001, SANS Top 20 and UK Cyber Essentials) before looking at practical guidance on how to choose the model and systems that are most appropriate for your organisation.

What attendees will learn:

- What some of the more common security models look like – and how those should change
- What some of the common security management systems are, and the key differences between them
- How to determine business requirements and map those on to the security management systems
- How to decide which security management systems are most appropriate for your organisation

PGI

Bridging the cyber skills gap – practical steps to building a roadmap

Steve Mair, Senior Cyber Security Consultant, PGI; and **Sebastian Madden,** Chief Corporate Development Officer, PGI

We all know there's a cybersecurity skills gap, and you already employ cyber specialists: you just don't know it yet (and the chances are that nor do they). In this session, you'll find out how to develop existing staff into cyber experts by going through some easy, practical steps. Your staff know your organisation and systems and can be taught cyber.

What attendees will learn:

- How to identify staff who can be cross skilled/ trained up to support cybersecurity challenges within their business
- How to explore where to look for information in terms of job roles/skills required for cyber capable staff
- How to develop an appropriate cyber skills framework to provide consistent measurement of progress
- How to retain staff, who might look elsewhere, by giving them a defined career path with measurable milestones and goals

Education Seminars	
Recorded Future **Best practices for applying threat intelligence** **Chris Pace,** Technology Advocate, Recorded Future	Threat intelligence is certainly one of the most talked-about areas of information security today. Recent research conducted by SC Media revealed that 46% of security professionals expect threat intelligence to be a very important part of their strategy in 2017. But when it comes time to choose threat intelligence services and products it can be hard to know where to start. During this session, we'll look at what types of intelligence will prove truly beneficial to your organisation and how to get the greatest return on your investment. What attendees will learn: • Best practices and case studies for implementing threat intelligence as part of your own information security strategy • Understand the important distinction between threat data and intelligence • Gain insight into the value of different intelligence sources and how to work with them • Learn about the importance of context in threat intelligence
SABSAcourses **Architecting a multi-tiered control strategy** **Charles Lewis,** Senior Consultant, SABSAcourses	Information Security departments are spending increasing amounts, and contributing more resources to standards compliance and security controls, but yet there's no guarantee of being safe and secure. Isn't the idea of security to avoid business disruption and ensure there is a robust, fit-for-purpose, business enabling and end-to-end solution? In this session, we will look at an engineered approach, applying some structured thinking through the SABSA Multi-Tiered Control Strategy to ensure information security contributes in a risk-proportional manner to the business. This defence-in-depth approach avoids concentrating only on limited best practices by looking at a more holistic approach to selecting capabilities to avoid business disruption. What attendees will learn: • What the SABSA Multi-Tiered Control Strategy looks like • How to identify the right type of control, in the right place and at the right time • How to incorporate, integrate and fully utilise existing control sets to build on current strengths and fill the gaps • How to respond in a risk-proportional manner, identifying weak links in the security chain
Thycotic **The evolving perimeter – where are the new boundaries?** **Joseph Carson,** Chief Security Scientist, Thycotic	The traditional security perimeter is proving to no longer be an effective cybersecurity control and fast growing technologies, such as cloud, mobile and virtualisation make the boundaries of an organisation blurry. For many years, organisations have protected their valuable and sensitive information by building a fence around assets, and all of the data that flowed in and out was either via a single internet access point or on physical devices. This meant that a traditional perimeter was an effective measure as the boundaries were known. As long as the internet access was controlled by the data that flowed through it, it was possible to protect, monitor and control that data. Organisations protected internet access with firewalls, VPNs, access controls, IDS, IPS, SIEMs, email gateways, and so forth, building multiple levels of security on the so-called perimeter. On physical devices, systems management and antivirus protected those systems and kept them updated with the latest security patches. This is a traditional security approach, used for nearly 30 years. However, in today's world it is no longer effective alone. The perimeter has moved and we need to move with it. What attendees will learn: During this session, attendees will learn about how identity and access management is evolving fast and becoming the new security perimeter, including: • Why the traditional perimeter is no longer effective • What hacker techniques are being used to compromise organisations • What some governments are doing to protect their citizens • Technologies that will help create the new cybersecurity perimeter