# 10th Annual e-Crime Dubai

March 20th, 2018, Dubai, UAE

## Securing the innovation economy

How new technology and new security policies can defend new digital models

e-crime & cybersecurity CONGRESS

www.akjassociates.com/event/dubai

AKJ Associates

# e-Crime Dubai 2018: securing innovation

"With the launch of the Dubai Cyber Security Strategy [we want to make] Dubai digitally the safest city in the world,"
His Highness Sheikh Mohammed Bin Rashid Al Maktoum Vice President and Prime Minister of the United Arab Emirates (UAE)
and ruler of the Emirate of Dubai

"Providing a robust platform for collection and sharing of cyber threat intelligence will allow banks to answer the 'who, what, where, when, why, and how' questions needed for immediate decisions and actions required," Abdul Aziz Al Ghurair, chairman of the UAE Banks Federation

Introduction

GCC organisations have been among the world's most rapid adopters of cybersecurity solutions in the face of the growing threat. One recent research report predicts that the GCC cybersecurity market will reach over $10.4 billion by the end of 2022.

Both public and private sectors continue to innovate. A new cyber security strategy for Dubai has just been launched by the UAE's Vice President and Prime Minister Dubai's ruler Sheikh Mohammed bin Rashid Al Maktoum as he also opened the Dubai Electronic Security Centre, which will deal with electronic security threats, cyberattacks and all forms of cybercrime.

These initiatives commit Dubai to focusing on securing the cyber-smart nation, establishing a cyber space that is "free, fair and secure", continuing to focus on protecting the confidentiality, credibility, availability and privacy of data, improving cyber-resilience and consolidating national and international collaboration. The next phase of the strategy will witness a "number of effective initiatives" that will contribute to providing a secure cyberspace.

In the private sector too companies continue to upgrade their defences. , the UAE Banks Federation has just launched the Middle East's first threat intelligence sharing platform for banks to counter a "sharp uptick" in cyber attack threats in the region. Initially, 13 banks of UBF will share cyber intelligence in a new UBF-ISAC, but later the platform will be extended to other banks and perhaps other sectors.

Continued innovation is required: the UAE is the region's financial hub and a centre for digital transformation. Emcredit, a subsidiary of Dubai Economy, and the UK-based Object Tech Group Ltd are working to create a blockchain-based digital currency, emCash, with merchants receiving payment in real time without going through intermediaries.

And billion-dollar e-Commerce website Noon.com has just started operations in the country.

All this digital transformation needs to be cyber-secure and UAE firms are keen for information on the latest techniques and technologies.

**The 10th e-Crime Information Security Dubai will cover these and other key subjects for its audience of professionals tasked with safeguarding digital assets and sensitive data. There will be real-life case studies, strategic talks and technical break-out sessions from security teams behind some of the world's most admired brands, who know, just like you, that security is now more important to business than ever before.**

Key Themes

# e-Crime Dubai 2018: Key themes

**Smart cities: the greatest cyber challenge yet**

- Securing an infinite attack surface
- Public versus private responsibility
- Where the Smart city meets the private enterprise: threat or opportunity?

**Getting the basics rights**

- Avoiding obvious configuration, patch and other errors
- Identifying and valuing critical assets
- Ensuring plans are fit for real-world deployment
- Best-practice incident response

**Securing e-Commerce**

- Symptoms, indicators, and red flags
- What does the data look like?
- EMV malware – how does it work and how to stop it?
- Defeating pre-paid card fraud schemes

**Automation is here – keeping up with explosive data and connectivity growth**

- How to automate and engineer out as many human decision points as possible
- Automated incident response – is AI the answer?
- Automating asset discovery and network intelligence
- Automated identity management

**Continuous security assessment and compliance**

- Maintaining security and compliance versus meeting snapshots
- Advanced network scanning and monitoring
- Automated mapping of security reports to key standards

**Improving web security**

- How many websites do you have? Auditing web presence and applications
- Advanced web attacks and exploitation
- Secure web application development
- Stopping SQL injection and XSS attacks once and for all

**Understanding Cloud and SaaS security – in-depth**

- The pros and cons of security as a managed service
- Maintaining control and visibility over Cloud data and applications
- Cloud vulnerability management
- Who is in charge of your Cloud?

**Machine learning and AI**

- What can AI do and what are its limitations?
- Where in the overall network and datasphere does AI make the most sense?
- Cognitive security versus machine learning

Demonstrate your solutions

# End-users and security professionals need your help …

## 1 To improve and automate network security

Automated asset discovery, configuration collection and change management; continuous, intelligent network scanning; whitelisting and blacklisting; automated patching. Clients need all this now. **This is the opportunity to showcase your solution.**

## 2 To secure the IoT

Managing the cybersecurity of industrial installations and connected infrastructure is no longer a fringe activity when everything is connecting. Key vendors are acquiring in this sector. **How can you help secure Smart?.**

## 3 To comply with regulations

Cyber-security is going mandatory. Voluntary commercial codes are not enough. Regulators want companies to demonstrate true cyber-security as well as basic compliance. **How can you help CISOs with this?**

## 4 To ensure web security

Too many companies still fall victims to 15-year-old techniques like SQL injection. Too many still find visibility into their web presence difficult. And that's before the real problems of secure web application development. **Can your products help?**

## 5 To secure payments and personal data

Financial services companies struggle with new and legacy systems, retailers struggle with PCI DSS, and everyone is worried about new payment methods such as contactless and phone. **Which solutions are available, scalable and easy to implement?**

## 6 To maximise Cloud security and efficiency

Realistically, most companies will migrate a majority of their IT to the Cloud. Resources and economies of scale will dictate it. This outsourced IT needs securing. Also, security itself will be outsourced to the Cloud. **How can you help with this transformation?**

Demonstrate your expertise

# They are looking for solutions in …

Mobile Security

## Priorities in securing mobile environments

The complexities of managing mobile security are increasing as more and more business and consumer activity migrates to mobile devices. How do you create trusted mobile environments? How do you ensure secure data backup for mobile devices? What are the best solutions for mobile threat defence? And what special considerations are needed for mobile application development and security testing?

Identity management

## Intelligence-driven security

Identity defined security is the next generation of IAM. It will allow for intelligence-based, risk-based, adaptive decision making in all aspects of cyber security. The end goal is that threats, breaches and incidents will be managed and contained more dynamically, and CISO's will be able to report on the health and well-being of the entire cyber security framework based on metrics from these integrations.

Cloud concerns

## Preparing for a Cloud-based future

Public cloud will be the prime delivery model for more than 60% of security applications by the end of 2017. CASBs continue to increase the urgency for control and viability of cloud services by addressing the gaps in security due to the increase in cloud service & mobile usage. So how do firms get visibiltiy and control over Cloud applications? How do they evaluate Cloud Access Security Brokers?

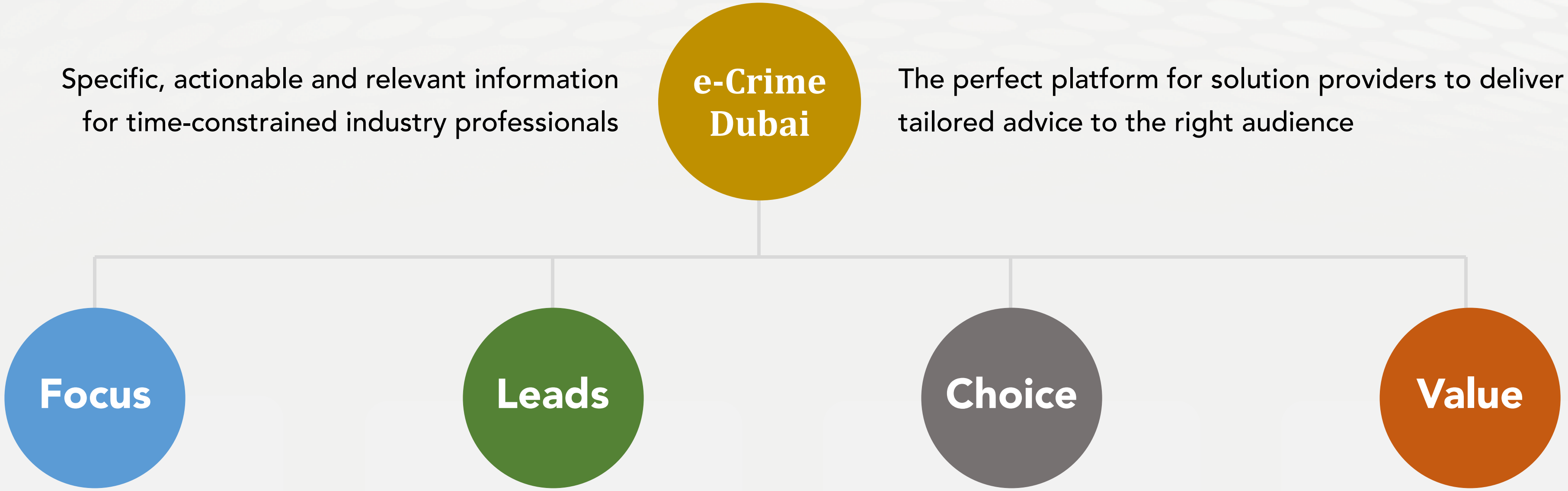
Endpoint detection & response

## Choosing an EDR solution

Managed endpoint detection and response solutions have been proposed as the defence against the problem of latency in traditional security systems. They increase visibility into endpoint status, actively block threats, monitor privileged accounts and even utilise machine learning to detect threats and malicious activity. So what kinds of organisations should adopt them? How much do they cost? And what improvements in their capabilities are being developed?

Where market-leading solution providers know they will find buyers

# We deliver a focused selling opportunity



Specific, actionable and relevant information for time-constrained industry professionals

e-Crime Dubai

The perfect platform for solution providers to deliver tailored advice to the right audience

Focus

Leads

Choice

Value

### Target growth

Each event represents a targeted opportunity to address the needs of a specific community whose need for your solutions and services is growing.

### Boost sales

Sponsors can tailor messages to the needs of an audience that shares similar concerns and challenges, looking for solutions now.

### Meet commercial aims

We work with sponsors to ensure they meet their commercial aims. We offer a number of sponsorship options, each providing specific benefits.

### Showcase solutions

Our events provide sponsors with a unique platform to showcase solutions, as well as provide advice on how best to solve delegates' key challenges.

Where the real decision-makers allocate budgets

# Why do so many blue-chip vendors work with us? Real buyers …

100% The most senior cyber-security solution buyers

You will be surrounded by the most senior buying audience in the cyber-security market.

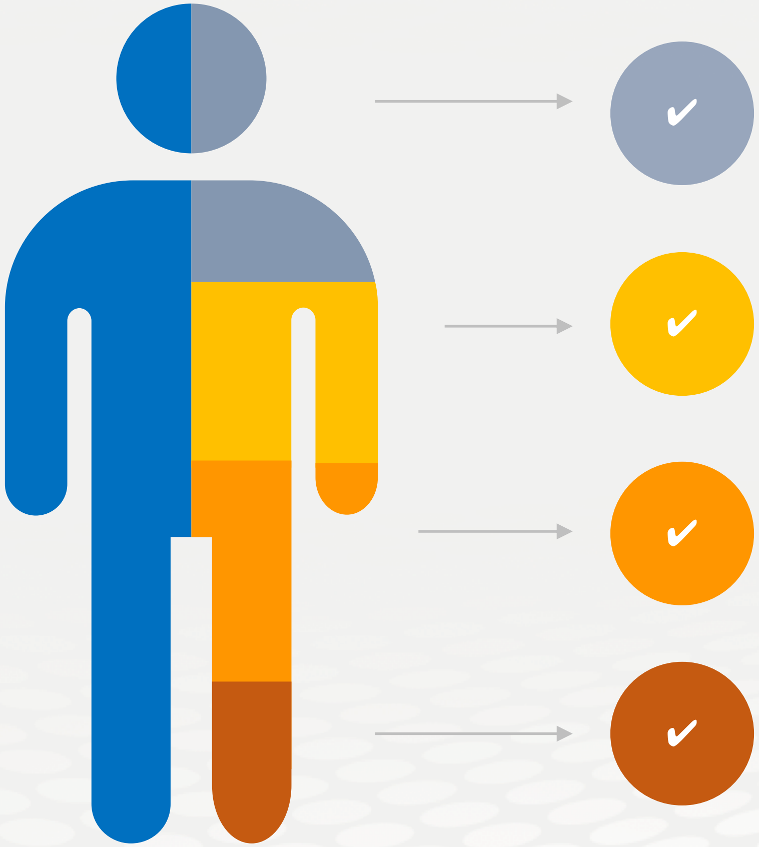
The AKJ Associates delegate database is the largest compilation of senior information risk and security professionals in the world. We have been building it since 1999!

We know the senior executives who drive strategy from the top, we know the enterprise architects who often control the largest budgets and we know the IT Security Leads and Engineers who so often dictate the purchase process.

All of these job titles attend the e-Crime Congress Dubai.

We understand that every vendor needs to sell more. That is the bottom line.

Getting in front of the right people at the right time always increases the lead generation and always increases profitable sales activity



### Cybersecurity

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

Where the top solution vendors get their message across

e-crime & cybersecurity CONGRESS

# Why do so many blue-chip vendors work with us? Real benefits…

## Talk to customers

Face-to-face interaction with the right buyers works! Our vendors tell us it does and they renew year after year

## Build relationships

Relationships built from a personal meetings are stronger than those initiated by solely digital conversations

## Save time

Meet dozens or hundreds of selected buyers in just one or two days – the value of a high quality event

## Lead sourcing

We provide the best leads in the business. Each sponsor receives a full delegate list at the end of the meeting

## Increase sales

All delegates are the right delegates. They have all been researched and confirmed as senior and with buying capacity

## Get your message across

Delegates take all lunches and breaks are in the exhibition. So sponsors and exhibitors are always surrounded by qualified buyers

Our testimonials speak for themselves: we have many more

e-crime & cybersecurity CONGRESS

# What our sponsors say about us

PHISHME

A great success. Organised and run with the usual AKJ friendliness and efficiency, we were very happy to have supported and will be pleased to attend again.

KASPERSKY lab

E-Crime UAE events have yet to disappoint – from the massive number of attendees to our packed speaking sessions, this is one event we always look forward to!

eset

We found the event very productive, it was good to meet potential customers and gives a chance for decision makers to meet us and understand what we do and how we can help them with their security.

**Ninety five percent of our exhibitors and sponsors work with us on a number of occasions each year.**

**Our sponsor renewal rate is unrivalled in the marketplace.**

**This is because our sponsors generate real business at our events every year**