e-Crime & Artificial Intelligence Forum

July 5th, 2018, London, UK

Are you ready for "cognification"?

Intelligent cybersecurity: cut costs, improve performance

e-crime & Artificial Intelligence Forum

www.akjassociates.com/event/ai

AKJ Associates

Introduction

e-Crime AI 2018: reduce costs, improve security

"The AI in security market is expected to be valued at USD3.92 billion in 2017 and to reach USD 34.81 billion by 2025, a CAGR of 31.38%."

"Addressing today's threats requires real-time Artificial Intelligence to scale your team of information security analysts across your entire enterprise."

As one analyst puts it, "The volume of threat data is exceeding the capacity of even the most skilled security professional, and organizations are drowning in a sea of information that continues to grow as rapidly as the threat landscape itself. When organizations see over 200,000 security events every day and don't have the skills to stay ahead, where do you turn?"

The answer, increasingly, in the use of AI-based solutions. Not only can automated, intelligent systems analyse volumes of data no humans can tackle, but they can spot patterns and anomalies far more quickly too

These abilities not only improve security, they lower its cost by reducing the number of analysts needed to manage the current crop of passive defences.

In combination with human analysts these systems are also far quicker and more accurate in identifying more complex threats and anomalies.

AI solutions now exist in network security, endpoint security, application security, and cloud security. Vendors exist who have applied machine learning to identity and access management (IAM), risk and compliance management, encryption, data loss prevention (DLP), unified threat management (UTM), antivirus/antimalware, intrusion detection/ prevention system (IDS/IPS), and pretty much every other area of cybersecurity – firewall, security and vulnerability management, disaster recovery, DDOS mitigation, web filtering, application white listing, and patch management.

Advanced AI and Machine Learning is helping analysts meet the volume and sophistication of modern attacks, reducing organizational risk, improving visibility and improving SOC teams' ability to stay ahead of modern threats.

But with so many vendors claiming AI expertise, how can CISOs evaluate the AI ecosystem? How do vendors differentiate?

The e-Crime AI Forum 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 to help end-users understand how these new technologies can be cost-effectively deployed in real-life business situations.

e-Crime & Artificial Intelligence Forum 2018: Key themes

Key Themes

Understanding AI, machine learning, deep learning and neural nets
- What exactly is Artificial Intelligence? What's the difference between machine learning, deep learning, neural nets, context awareness computing, and natural language processing?
- What can it do better than humans and what does it do worse?

Evaluating AI and machine learning solutions
- How do their AI engines differ?
- What are they good at and what are they bad at?
- What questions should you ask an AI vendor?

AI in core network security
- Automating asset discovery and network intelligence
- Is AI plus human analysts the optimum combination?
- What about the endpoints?

AI in alert prioritization and data analysis
- Separate the signal from the noise
- Automating incident response
- Is AI plus human analysts the optimum combination?
- Automating the SOC

AI in identity and access management
- Detecting Shared Logins and User Credentials
- Third-Party Access Data Compromise
- Privileged User Account Abuse
- Geolocation and Remote Access Security

AI's role in defending against malicious insiders
- Accurately identify malicious insiders from user behaviours
- Detecting data snooping
- Predicting employee departure and preventing data exfiltration

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

Deploying AI solutions
- What is the difference between deploying AI versus conventional solutions?
- How much training / data do you need for the solution to work?
- Are AI solutions more difficult to maintain or scale?

Demonstrate your solutions

End-users and security professionals need your help with improved intelligence and proactive threat hunting ….

1 To automate network security

Configuration collection and change management; continuous, intelligent network scanning; whitelisting and blacklisting; automated patching. **This is the opportunity to showcase your solution.**

2 To build next generation SOCs

How can CISOs meet the volume and sophistication of modern attacks, reduce organizational risk and improve SOC teams' ability to stay ahead of modern threats? **Do your AI solutions help?**

3 To improve network and threat visibility

AI promises true visibility into network traffic, anomaly detection and attack patterns, guiding analysts to the most critical answers that support faster response times. **How can you help CISOs with this?**

4 To solve the IDAM problem

AI solutions say they can deliver advanced "intelligent" dynamic access control technology to effectively block hacking, ID theft, rogue digital intrusion and user impersonations once and for all. **Can your products help?**

5 To secure web applications

New web application firewalls leverage AI to dynamically and automatically update security postures to protect web applications from vulnerabilities. **Which solutions are available, scalable and easy to implement?**

6 To detect and prevent the latest email attacks

Machine learning models can analyse billions of emails, use identity mapping, trust models and behavioural analytics to spot sophisticated phishing attacks. **Are these a key part of the solution to the human problem?**

They are looking for solutions in …

Demonstrate your expertise

SIEM

Solving the problem of false positives

SIEM systems generate too many false positive alerts, making it difficult for analysts to detect and mitigate real threats quickly. But AI threat detection, when not implemented carefully, can generate even more false positives, further eroding the effectiveness of Security Operations Center (SOC) analysts. So what combination of machine learning and big data architecture provide a solution?

Identity management

Smarter ways to guard the network

First there were passwords; then there was IAM analytics. But examining logs to ID suspicious behavior has become increasingly difficult with multiplying endpoints and legitimate user behavours. AI promises “intelligent” dynamic access control technology to effectively block hacking, ID theft, rogue digital intrusion and user impersonations once and for all. Does it work?

Intrusion & detection systems

Managing scale, prioritizing threats

Sophisticated attackers can bypass traditional defences techniques, so the need for more intelligent intrusion detection is increasing by the day. Machine learning is one answer but such solutions need large and robust data sets to provide examples from which the computer can learn. Today, however, very little security data is publicly available. So how do these solutions work?

Cognitive endpoint protection

Choosing an intelligent 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 AI Forum

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

Focus

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.

Leads

Boost sales

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

Choice

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.

Value

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 and most sophisticated buying audience in the cybersecurity 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 cybersecurity 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

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

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