

# Post event report



The 15<sup>th</sup> e-Crime & Cybersecurity Congress in Abu Dhabi

4<sup>th</sup> September 2024 | Abu Dhabi, UAE

## Principal Keynote Sponsor



## Strategic Sponsors



## Education Seminar Sponsors



## Networking Sponsors



“ I wanted to take a moment to share my excitement about the recent Cybersecurity Congress me and my colleague attended. The event was truly remarkable and left me thoroughly impressed. From the insightful keynote speeches to the engaging breakout sessions, every aspect of Congress was designed to deepen our understanding of current cybersecurity challenges and advancements. The opportunity to interact with industry leaders and experts was invaluable, and I came away with a wealth of knowledge and innovative ideas that I am eager to apply. Thank you for organising such a high-caliber event. It was an incredible experience, and I look forward to future opportunities to collaborate and learn more from this dynamic field. ”

IT Head, AI Fuad Exchange

“ I had the privilege of attending the AKJ Associates Cybersecurity Conference in Abu Dhabi. The presentations were insightful, especially on leveraging AI for cyber-defence and exploring practical solutions for risk management. The panel discussions fostered rich dialogues on the evolving threat landscape and regulatory challenges. This conference gave me an opportunity to have an overview of the recent trends, threats, and products/solutions around cybersecurity. Overall, the event offered valuable, actionable takeaways for professionals aiming to enhance their organisations' cybersecurity posture. ”

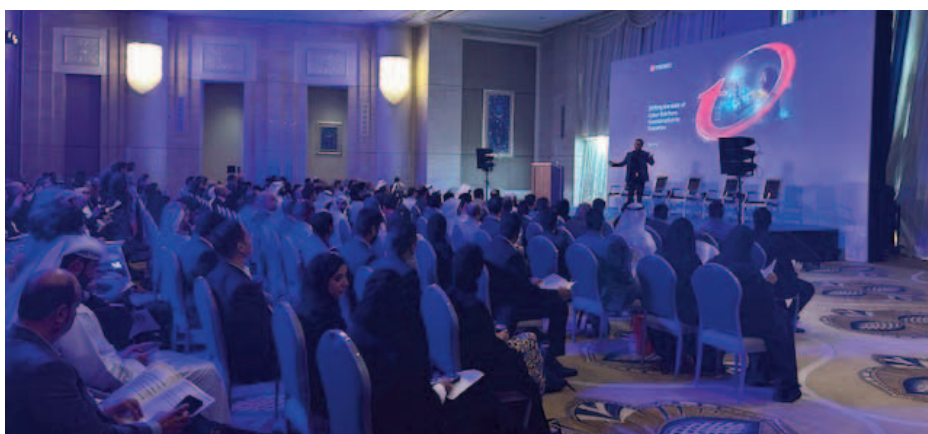
Senior Internal Auditor, Yahsat

“ I was given the privilege to attend the e-Crime & Cybersecurity Congress held at St. Regis Abu Dhabi, and it was an exceptional experience. Professionals, experts and leaders in the field were brought together giving invaluable insights into the latest cybersecurity trends and challenges. The speakers were highly knowledgeable and shared real-world strategies and solutions to combat evolving cyber-threats which I can immediately apply to my work. Overall, the event was well-organised, informative and a must attend to everyone who wanted to be on top in the cybersecurity field. ”

Compliance Manager, State Street Corporation

Inside this report:

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



### Speakers

Dr Ebrahim Al Alkeem, Cybersecurity and Artificial Intelligence Director, **Abu Dhabi Government**

Mamdouh Al-Gendy, Senior Technology Consultant, **Entrust**

Hussain Al Khalsan, CISO, **ZAND**

His Excellency Dr. Mohamed Al Kuwaiti, Head of Cybersecurity, **United Arab Emirates Government**

Sultan Al Mansoori, Director of Information Security, **Abu Dhabi Media (ADM)**

First Lieutenant Nasser Al Neyadi, Head of Information Security Department, **Ministry of Interior**

Khaled Al Teneiji, Cybersecurity Head, **ENOC**

Aus Alzubaidi, CISO, Director of IT & Media, **MBC Group**

Ara Antoun, Chief Operations officer, **MEInfoSec**

Bilal Baig, Technical Director, MMEA, **Trend Micro**

Simon Brady, Editor, **AKJ Associates**

Michael Byrnes, Director, Solutions Engineering META, **BeyondTrust**

Mohamed Djenane, Sr. Director Sales Engineering MENA/APAC, **Seclore**

Anoop Kumar, Head of Information Security Governance Risk and Compliance, Gulf News, **Al Nisr Publishing**

Alexey Lukatsky, Managing Director, **Positive Technologies**

Gary Pollock, Solutions Engineering Manager, **CyberArk**

Meenakshisundaram Ramakrishna Sahadevan, Product Marketing Analyst, **ManageEngine**

Hafeez Rehman, Group Manager, Security Consultant Team, **Kaspersky**

Manit Sahib, Ethical Hacker, **The Global Fund**

Hussein Hassan Shafik, Group CISO and Privacy Officer, **Abu Dhabi Islamic Bank**

Zaheer Mubarak Shaikh, CISO, **Al Maryah Community Bank**

Vikalp Shrivastava, Global CISO, **Kerzner International**

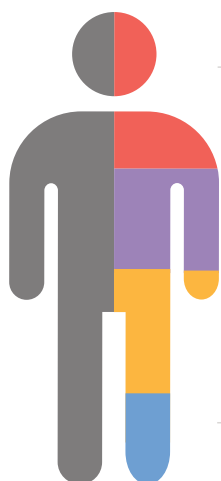
John Smith, EMEA CTO, **Veracode**

Rajesh Yadla, Head of Information Security, **Al Hilal Bank**

### Key themes

- Upgrading legacy cybersecurity stacks
- Balancing multiple point solutions with one-stop shops
- Using AI and ML to automate cybersecurity
- Insuring the uninsurable?
- Cybersecurity for SaaS/laaS/PaaS
- Upskilling security teams
- The rise and rise of effective cybersecurity regulation
- From smart machines to smart cities - securing the IoT
- Developing the next generation of security leaders
- Keeping citizens safe
- Reining in BigTech
- Securing digital currencies and DLT

### 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					
08:20	Breakfast & networking break				
09:20	Chairman's welcome				
09:30	<b>Opening keynote: Building a resilient cybersecurity culture</b> <b>His Excellency Dr. Mohamed Al Kuwaiti</b> , Head of Cybersecurity, United Arab Emirates Government <ul style="list-style-type: none"> <li>Emerging threats and trends</li> <li>Innovative solutions and technologies</li> <li>Building a resilient cybersecurity culture</li> </ul>				
10:00	<b>The new age cyber-threats: Leveraging AI to improve cybersecurity</b> <b>First Lieutenant Nasser Al Neyadi</b> , Head of Information Security Department, Ministry of Interior <ul style="list-style-type: none"> <li>Understanding the landscape of new age cyber-threats and the role of AI in identifying and mitigating these threats</li> <li>Implementing AI-driven solutions to enhance threat detection and response capabilities in real-time</li> <li>Integrating AI technologies into existing cybersecurity frameworks to bolster defences against sophisticated cyber-attacks</li> <li>Developing a strategic approach to continuous learning and adaptation, ensuring AI tools evolve alongside emerging threats</li> </ul>				
10:20	<b>Shifting the state of cyber-risk from guesstimation towards causation</b> <b>Bilal Baig</b> , Technical Director, MMEA, Trend Micro <ul style="list-style-type: none"> <li>The content will focus on the transition from isolated security measures to a unified framework, with a special emphasis on the effectiveness of Zero Trust Architecture</li> </ul>				
10:40	<b>Education Seminars   Session 1</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;"> <b>MEInfoSec</b>  <b>The real risk – Why patching is still a challenge</b>  <b>Ara Antoun</b>, Chief Operations officer, MEInfoSec                         </td> <td style="width: 33%; padding: 5px;"> <b>Positive Technologies</b>  <b>The business model of modern cybercrime: A new look or why the black market will never disappear?!</b>  <b>Alexey Lukatsky</b>, Managing Director, Positive Technologies                         </td> <td style="width: 33%; padding: 5px;"> <b>Veracode</b>  <b>From data to done: Remediating the app risk that matters most, with the least amount of effort</b>  <b>John Smith</b>, EMEA CTO, Veracode                         </td> </tr> </table>		<b>MEInfoSec</b> <b>The real risk – Why patching is still a challenge</b> <b>Ara Antoun</b> , Chief Operations officer, MEInfoSec	<b>Positive Technologies</b> <b>The business model of modern cybercrime: A new look or why the black market will never disappear?!</b> <b>Alexey Lukatsky</b> , Managing Director, Positive Technologies	<b>Veracode</b> <b>From data to done: Remediating the app risk that matters most, with the least amount of effort</b> <b>John Smith</b> , EMEA CTO, Veracode
<b>MEInfoSec</b> <b>The real risk – Why patching is still a challenge</b> <b>Ara Antoun</b> , Chief Operations officer, MEInfoSec	<b>Positive Technologies</b> <b>The business model of modern cybercrime: A new look or why the black market will never disappear?!</b> <b>Alexey Lukatsky</b> , Managing Director, Positive Technologies	<b>Veracode</b> <b>From data to done: Remediating the app risk that matters most, with the least amount of effort</b> <b>John Smith</b> , EMEA CTO, Veracode			
11:20	Networking break				
11:50	<b>EXECUTIVE PANEL DISCUSSION   CISO daily challenges</b> <b>Simon Brady</b> , Event Chairman, AKJ Associates (Moderator); <b>Hussain Al Khalsan</b> , CISO, ZAND; <b>Rajesh Yadla</b> , Head of Information Security, Al Hilal Bank; <b>Sultan Al Mansoori</b> , Director of Information Security, Abu Dhabi Media (ADM); <b>Khaled Al Teneiji</b> , Cybersecurity Head, ENOC; <b>Hussein Hassan Shafik</b> , Group CISO and Privacy Officer, Abu Dhabi Islamic Bank <ul style="list-style-type: none"> <li>What are your biggest challenges in the day-to-day battle of protecting your customers and organisation? What threats worry you the most?</li> <li>Security versus resilience: aligning security priorities with organisational objectives. How do you prioritise, and do you feel supported and heard when airing concerns?</li> <li>How do you assess and prepare for the threat of state-sponsored cyber-attacks targeting your organisation? What strategies do you have in place to ensure cloud security and manage associated risks?</li> <li>In the event of a significant cyber-incident, what are the key components of your incident response strategy, and how do you ensure that your organisation can quickly recover and continue operations?</li> <li>With the regulatory environment continually evolving, and with new data protection laws and cybersecurity regulations being introduced, how do you ensure your organisation remains compliant with both local and international regulations, and what challenges does this bring?</li> <li>What initiatives have you implemented to promote cybersecurity awareness and ensure that security practices are integrated into the daily activities of all employees?</li> <li>How are you addressing the challenges of attracting, developing, and retaining skilled cybersecurity professionals in your organisation?</li> </ul>				
12:20	<b>Understanding AI's impact on securing privileged identities</b> <b>Michael Byrnes</b> , Director, Solutions Engineering META, BeyondTrust <ul style="list-style-type: none"> <li>As a matter of fact, AI is THE new buzzword, and it comes with its set of new opportunities and capabilities for cybercriminals – which is even more concerning because their AI systems are designed to learn and improve over time. Criminals who train their own AI systems on malware and other malicious software can significantly 'level up' their attacks.</li> <li>What is the effect of AI threats on identity security, including real-life examples?</li> <li>How does AI impact the identity attack chain?</li> <li>What are the key tips for safeguarding your organisation from emerging threats?</li> </ul>				

Agenda		
<b>12:40</b>	<b>Embracing crypto agility: Future-proofing security in the UAE</b>	
	<p><b>Mamdouh Al-Gendy</b>, Senior Technology Consultant, Entrust</p> <p>Crypto agility is an essential strategy for maintaining robust security in an evolving threat landscape. Learn how to future-proof your organisation's security infrastructure, ensuring resilience against both current and future cyber-threats. Discover best practices and real-world case studies on how to support your journey towards crypto agility and post-quantum cryptography. Attendees will learn:</p> <ul style="list-style-type: none"> <li>• The fundamentals of crypto agility</li> <li>• Its importance in addressing emerging cryptographic threats now</li> <li>• Practical steps for implementing agile cryptographic solutions, including the impact on your PKI, certificate lifecycle management, data security and compliance</li> </ul>	
<b>13:00</b>	<b>Education Seminars   Session 2</b>	
	<p><b>CyberArk</b></p> <p><b>QR codes in a post pandemic world</b></p> <p><b>Gary Pollock</b>, Solutions Engineering Manager, CyberArk</p>	<p><b>ManageEngine</b></p> <p><b>Vault and beyond: A life cycle approach to AI-powered privileged access management</b></p> <p><b>Meenakshisundaram Ramakrishna Sahadevan</b>, Product Marketing Analyst, ManageEngine</p>
		<p><b>Seclore</b></p> <p><b>A harmless breach – Is it the future of cybersecurity?</b></p> <p><b>Mohamed Djenane</b>, Sr. Director Sales Engineering MENA/APAC, Seclore</p>
<b>13:40</b>	Lunch & networking break	
<b>14:40</b>	<b>Enhancing cybersecurity through effective cyber-governance and regulation</b>	
	<p><b>Anoop Kumar</b>, Head of Information Security Governance Risk and Compliance, Gulf News, Al Nisr Publishing</p> <ul style="list-style-type: none"> <li>• How do we effectively integrate cyber-governance into our corporate strategy?</li> <li>• Navigating regulatory compliance and standards</li> <li>• Are public-private partnerships the way to enhanced security for all?</li> </ul>	
<b>15:00</b>	<b>Cyber-threat intelligence – strategic, operational, and tactical ... take your cyber-defence and resiliency to the next level</b>	
	<p><b>Hafeez Rehman</b>, Group Manager, Security Consultant Team, Kaspersky</p> <ul style="list-style-type: none"> <li>• Empower your cyber-defence arsenal with the intelligence to find the hidden threat, improve strategic and tactical decision-making, and elevate the posture of the digital risk plan</li> </ul>	
<b>15:20</b>	<b>FIRESIDE CHAT – A CISO's view: IPOs, ESG, and regulatory landscape</b>	
	<p><b>Simon Brady</b>, Event Chairman, AKJ Associates; <b>Aus Alzubaidi</b>, CISO, Director of IT &amp; Media, MBC Group</p> <ul style="list-style-type: none"> <li>• What are the key cybersecurity measures a company should implement before going public to ensure investor confidence and compliance with regulatory requirements?</li> <li>• How can companies identify and mitigate cyber-risks that could impact their valuation or delay the IPO process?</li> <li>• What role do cybersecurity audits and due diligence play in the IPO preparation phase?</li> <li>• How does cybersecurity intersect with ESG criteria, and why is it crucial for companies to integrate cybersecurity practices into their ESG strategies?</li> <li>• How do strong cybersecurity measures contribute to the social and governance aspects of ESG?</li> <li>• How are investors and stakeholders increasingly viewing cybersecurity as a critical component of a company's overall ESG performance?</li> <li>• How can companies stay updated with evolving cybersecurity regulations and ensure ongoing compliance?</li> <li>• Are regulations fit for purpose? Do potential penalties and consequences for non-compliance with cybersecurity regulations really act as a deterrent?</li> </ul>	
<b>15:40</b>	Networking break	
<b>16:00</b>	<b>EXECUTIVE PANEL DISCUSSION   Embracing AI: A double-edged sword</b>	
	<p><b>Simon Brady</b>, Event Chairman, AKJ Associates (Moderator); <b>Dr Ebrahim Al Alkeem</b>, Cybersecurity and Artificial Intelligence Director, Abu Dhabi Government; <b>Zaheer Mubarak Shaikh</b>, CISO, Al Maryah Community Bank; <b>Manit Sahib</b>, Ethical Hacker, The Global Fund; <b>Vikalp Shrivastava</b>, Global CISO, Kerzner International</p> <ul style="list-style-type: none"> <li>• What are the primary advantages you see in integrating AI into your organisation's cybersecurity framework, and how have these benefits manifested so far?</li> <li>• What challenges have you encountered while implementing AI-driven cybersecurity solutions, and how have you addressed these obstacles?</li> <li>• How do you ensure the reliability and accuracy of AI algorithms in identifying and mitigating cyber-threats?</li> <li>• What measures do you take to prevent and mitigate AI-specific risks, such as adversarial attacks or AI system vulnerabilities?</li> <li>• How do you balance the deployment of AI technologies with the need for human oversight and expertise in your cybersecurity operations?</li> <li>• What strategies do you use to address the ethical and privacy concerns associated with the use of AI in cybersecurity?</li> <li>• Looking ahead, what future AI advancements or trends are you most excited about, and how do you plan to integrate these into your cybersecurity strategy?</li> </ul>	
<b>16:30</b>	<b>LIVE DEMONSTRATION: Weaponising AI for cyber-attacks &amp; offensive operations</b>	
	<p><b>Manit Sahib</b>, Ethical Hacker, The Global Fund</p> <ul style="list-style-type: none"> <li>• Overview &amp; threat landscape: How AI is being leveraged in the wild for malicious activities</li> <li>• Weaponising AI for offensive operations: Running AI through the cyber kill chain</li> <li>• ChatGPT or [insertnamehere]GPT: What's the level of effort required to build your own AI?</li> <li>• LIVE DEMO: AI in action</li> </ul>	
<b>16:50</b>	<b>Time for security to grow up</b>	
	<p><b>Simon Brady</b>, Editor, AKJ Associates</p> <ul style="list-style-type: none"> <li>• Current security models and attitudes are not fit for purpose</li> <li>• Organisations need to change their approach</li> <li>• Software firms must take responsibility for their products</li> <li>• Information sharing should be the norm not secrecy</li> <li>• Boards must walk the walk not just talk the talk</li> </ul>	
<b>17:00</b>	Conference close	

Education Seminars	
<p><b>CyberArk</b></p> <p><b>QR codes in a post pandemic world</b></p> <p><b>Gary Pollock</b>, Solutions Engineering Manager, CyberArk</p>	<p>QR codes were all but dead until smartphone companies started incorporating QR code scanners into their mobile phones back in 2017. Enter the COVID19 pandemic and the rise of the contactless economy, and the QR code is making a massive comeback. From advertising and restaurant menus to healthcare and agriculture – the use cases for QR codes are infinite.</p> <p>QR codes are accessible, easy to produce and seemingly, here to stay. They're also a perfect way for cybercriminals to snag your employee's personal information.</p> <p><b>Attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• Examples of three simulated QR code attacks</li> <li>• Tactics, Techniques, and Procedures (TTPs) used by QR code attackers</li> <li>• Ways to protect yourself and your employees</li> <li>• Implications for enterprise security teams and controls to have in place to prevent privilege escalation and lateral movement within the IT estate</li> </ul>
<p><b>ManageEngine</b></p> <p><b>Vault and beyond: A life cycle approach to AI-powered privileged access management</b></p> <p><b>Meenakshisundaram Ramakrishna Sahadevan</b>, Product marketing analyst, ManageEngine</p>	<p>Traditional PAM implementations often place a firm focus on the solution itself, neglecting the broader context of privileged access management. However, it is important to adopt a holistic approach that encompasses the entire life cycle of privileged users, right from onboarding to offboarding.</p> <p>By integrating AI-driven insights from across enterprise IT solutions, organisations can incorporate privileged access management best practices using AI-powered insights to mitigate risks and improve operational efficiency.</p> <p><b>Attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• The limitations of a traditional approach to privileged access management</li> <li>• How an integrated approach can help leverage AI insights throughout the privileged access lifecycle from across enterprise IT solutions</li> <li>• Tangible benefits and the way ahead</li> </ul>
<p><b>MEInfoSec</b></p> <p><b>The real risk – Why patching is still a challenge</b></p> <p><b>Ara Antoun</b>, Chief Operations officer, MEInfoSec</p>	<p>Patch management is a critical aspect of maintaining the security and functionality of software systems. However, it comes with a range of challenges that can make the process complex and difficult. Third-party applications are a significant vector for potential infections. The challenge today is how to minimise the risk and remediate the vulnerabilities. Effective patch management tools are essential for ensuring security, stability and continuity in an organisation's digital infrastructure. It also requires a balanced approach combining timely response with careful prioritisation. DarkSight resolves this issue and makes the patch management process more efficient.</p> <ul style="list-style-type: none"> <li>• 3rd party applications the root cause of infections</li> <li>• Regional top vulnerable applications and their impact</li> <li>• Challenges of patching and examples</li> <li>• DarkSight – identification and remediation</li> </ul>
<p><b>Positive Technologies</b></p> <p><b>The business model of modern cybercrime: A new look or why the black market will never disappear?!</b></p> <p><b>Alexey Lukatsky</b>, Managing Director, Positive Technologies</p>	<ul style="list-style-type: none"> <li>• Modern cybercrime operates like any market or business, but it is illegal?</li> <li>• We should analyse cybercriminals through the lens of economic principles</li> <li>• The business model of any enterprise, including cybercrime, consists of nine key components: key activities, key resources, partner networks, value propositions, customers, channels, customer relationships, cost structure, and revenue streams (with many examples of cybercrime products, services, and offers, particularly in the MENA region)</li> <li>• We can predict emerging cybercrime businesses by understanding these components</li> <li>• To effectively combat cybercrime, we must understand its business model and how we can disrupt it</li> </ul>

Education Seminars	
<p><b>Seclore</b></p> <p><b>A harmless breach – Is it the future of cybersecurity?</b></p> <p><b>Mohamed Djenane</b>, Sr. Director Sales Engineering MENA/APAC, Seclore</p>	<p>Data breach now average \$8 million in damages. But what if your data could stay secured even when compromised or exfiltrated? We often think of data breaches as inevitably catastrophic. But a new data-centric model questions this assumption and outlines a path toward a future where breaches become harmless.</p> <p><b>Attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• Transform your cybersecurity approach: Discover how data-centric security models can render data breaches harmless, even when compromised</li> <li>• Gain competitive advantage: Hear real-world success stories of companies that have turned breaches into harmless events, giving them an edge in the market</li> <li>• Stay ahead of trends: Get insights into future cybersecurity trends and prepare your organisation for the evolving threat landscape.</li> </ul>
<p><b>Veracode</b></p> <p><b>From data to done: Remediating the app risk that matters most, with the least amount of effort</b></p> <p><b>John Smith</b>, EMEA CTO, Veracode</p>	<p>Security teams today are grappling with a host of challenges that hinder their ability to manage their security risk posture effectively. From infrastructure and security tool sprawl, teams are missing a total view of risk, drowning in alert fatigue making it difficult to know how to prioritise and remediate at the pace business requires.</p> <p><b>Attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• Automated root cause analysis to tackle the most urgent and impactful application and cloud security issues</li> <li>• To ensure your organisation stays ahead of potential threats</li> <li>• To unify findings across development, build, deployment, and production tools</li> <li>• Provide comprehensive risk visibility from code-to-cloud and boost remediation velocity by 10x</li> <li>• Prioritise solutions based on the reduction of asset and identity risk</li> <li>• Cut remediation time by 75%</li> </ul>