Post event report

e-crime & cybersecurity CONGRESS

The 16th e-Crime & Cybersecurity Congress in Abu Dhabi

10th September 2025 | Abu Dhabi, UAE

Strategic Sponsors

DEFA3 CYBERSECURITY

Delinea Securing identities at every interaction

GROUP-IB

rubrik

SECLORE

THREATLOCKER

Education Seminar Sponsors

BeyondTrust

CHECK POINT

DARKSIGHT

fileorbis

Green Method

infoblox

invicti 100% Signal. 0% Noise.

ManageEngine

MEInfoSec Empowering IT Security

netskope

opentext

positive technologies

sectona

SILENT PUSH

VERACODE

Networking Sponsors

BULWARK Technologies

corelight

CYBERARK THE IDENTITY SECURITY COMPANY

CYBLE

Gulf IT Network Distribution

iZOOlogic

mimecast

Ping Identity

Recorded Future

SECURE DOMAINS

SPIRE INFORMATION. SECURED.

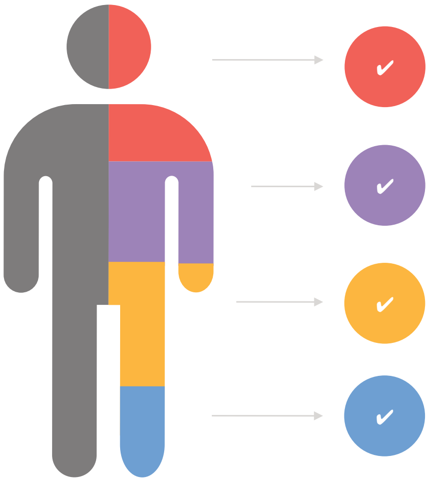
xage SECURITY

Inside this report:

Key themes

- Making the best use of threat intelligence
- Security posture management
- AI, quantum and the rest
- Improving continuous attack surface discovery
- The power of automation
- Adversary simulation and behavioural analysis
- Pen testing for OT / SCADA
- Why zero trust, isolation and segmentation are key
- OT and the regulations
- Defending against the latest ransomware variants
- Transitioning OT to the Cloud?
- Achieving visibility across ecosystems

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

Hani Abdel Karim Bani Amer, Head of Information Security, Al Etihad Payments

Hammam Abunaser, Sales Director – MEA, FileOrbis

H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security, UAE

Khaled Al Teneiji, Cybersecurity Head, ENOC

Luke Angus, VP EMEA, Silent Push

Ara Awakian, Chief Operations officer, ME InfoSec

Minas Awakian, Managing Director, ME InfoSec

Sameer Basha, Lead Sales Engineer & Evangelist, Check Point Software Technologies

Olivier Bussolini, Group CISO, Mashreq Bank

Mohamed Djenane, Senior Director Sales Engineering MEA, Seclore

Abdallah El Attar, Senior Solutions Architect, Infoblox

Ahmed Faragallah, Solutions Architect, Infoblox

Hussein Hassan Shafik, Group CISO, Abu Dhabi Islamic Bank

Michael Hughes, Senior Principal Customer Success Manager, Veracode

Philip Intallura, Group Head of Quantum Technologies, HSBC

Dominic Keating, Regional Director, Middle East and Türkiye, Rubrik

Benedict Kite, Defence, Security and Cyber Adviser, Kearney

Ashraf Koheil, Vice President Global Sales, Group-IB

Ilya Leonov, Regional Director MENA, Positive Technologies

Kamlesh Luhana, Senior Solutions Engineer, Netskope

Javeria Malik, Solution Engineer, Sectona

Salim Menikh, Sales Manager, OpenText

Zaheer Mubarak Shaikh, CISO, Al Maryah Community Bank

Kousain Raza, Senior Solutions Engineer, Netskope

Nick Roy, Sales Engineer, Silent Push

Manit Sahib, Ethical Hacker, Cytadel & Former Head of Penetration Testing & Red Teaming, Bank of England

Khaled Saleh, Regional Sales Manager – MEA Region, OpenText

Omar Samhouri, Senior Sales Engineer, Delinea

Rob Standing, Regional Vice President, Middle East, Africa and Türkiye, Rubrik

Igor Stolyarov, Business Development Manager, Group-IB

Vishal Thakkar, Director – Customer Success, Sectona

Julian Totzek-Hallhuber, Senior Principal Solution Architect, Veracode

Praneeth Vanteru, Technical Consultant, ManageEngine

Vijay Antony Velayutham, Principal Information Security Officer, UAE Ministry of Energy & Infrastructure

Rajesh Yadla, Head of Information Security, Leading Digital Bank

Bader Zyoud, Head of Information Security Governance and Risk Management, Abu Dhabi

Agenda

08:00	Breakfast & networking break
08:50	Chair's welcome remarks
09:00	**Digital revolution: The rise of cybersecurity** **H.E. Dr. Mohamed Al Kuwaiti,** Head of Cyber Security, UAE Topics covered in this presentation will include: • Cyber technologies and the balance of power • Cybersecurity as a national priority • Public–private collaboration • Emerging technologies and cybersecurity • The UAE model for secure digital transformation
09:20	**Disruptive technologies – Transforming the cybersecurity landscape** **Ashraf Koheil,** Vice President Global Sales, Group-IB; **Igor Stolyarov,** Business Development Manager, Group-IB • Real-world examples of how these technologies are being leveraged to detect, prevent, and respond to cyber-threats more effectively • The risks and challenges these technologies introduce – including how threat actors are also adopting them • Insights into future trends and how organisations can adapt their security frameworks to stay ahead of evolving threats
09:40	**Cybersecurity horizon scan in the UAE** **Hussein Hassan Shafik,** Group CISO, Abu Dhabi Islamic Bank • Major factors contributing to cybersecurity threats in the UAE • Cyber-threat landscape multipliers: Scope, Speed and Scale • Cyber-threat impact on people, process and technology • Scanning the horizon: What can be done? • Case example: FSIs in UAE and how we created a roadmap for cyber horizon risk
10:00	**How Delinea assists in reducing identity-related cybercrimes** **Omar Samhouri,** Senior Sales Engineer, Delinea • The landscape of existing PAM solutions • Switch from traditional PAM to a modern identity-centric solution • Reducing attack surface across the organisation • The use of AI in identity security
10:20	**Education Seminars | Session 1** **Infoblox** **The overlooked risk: Why DNS is the new frontline in cyber-defence** **Ahmed Faragallah,** Solutions Architect, Infoblox & **Abdallah El Attar,** Senior Solutions Architect, Infoblox **Netskope** **Securing data flow for the next wave of the AI era** **Kousain Raza,** Senior Solutions Engineer, Netskope & **Kamlesh Luhana,** Senior Solutions Engineer, Netskope **OpenText** **Re-imagine data privacy and protection in the AI era** **Khaled Saleh,** Regional Sales Manager – MEA Region, OpenText & **Salim Menikh,** Sales Manager, OpenText **Positive Technologies** **Desert Dexter: The hidden cyber-threat in the Middle East** **Ilya Leonov,** Regional Director MENA, Positive Technologies
11:00	Networking break
11:30	**FIRESIDE CHAT** **Strengthening Business resilience through proactive threat intelligence** **Benedict Kite,** Defence, Security and Cyber Adviser, Kearney; **Hani Abdel Karim Bani Amer,** Head of Information Security, Al Etihad Payments; **Khaled Al Teneiji,** Cybersecurity Head, ENOC • Turning complex data into clear, actionable threat insights to support strategic decisions • Using threat intelligence to anticipate and mitigate risks before they disrupt business operations • Embedding cyber-intelligence into broader operational resilience and risk management ecosystems • Enhancing cross-functional collaboration by aligning threat intelligence with enterprise risk priorities
12:00	**Securing tomorrow: The critical path to cyber-resilience** **Dominic Keating,** Regional Director, Middle East and Türkiye, Rubrik; **Rob Standing,** Regional Vice President, Middle East, Africa and Türkiye, Rubrik • In an era where nearly 90% ransomware incidents involve data exfiltration and extortion, nearly two in three companies report their data growth has exceeded their ability to secure it • Join senior executives from Microsoft and Rubrik as they dissect the complexities of modern cyber-threats, including the rise of triple-extortion attacks and evolving regulatory demands

Agenda

12:20 **Education Seminars | Session 2**

BeyondTrust	FileOrbis	Sectona	Veracode
BeyondTrust: The impact of AI in identity security **Theshan Mudaly,** Senior Solutions Engineer, BeyondTrust & **Saranraj Balaraman,** Partner Solutions Engineer, BeyondTrust	**Why data security falls apart without document security: The risk you can't afford to ignore** **Hammam Abunaser,** Sales Director – MEA, FileOrbis	**From control to confidence: The new era of modern infrastructure access** **Javeria Malik,** Solution Engineer, Sectona & **Vishal Thakkar,** Director – Customer Success, Sectona	**Is AI generated code secure?** **Julian Totzek-Hallhuber,** Senior Principal Solution Architect, Veracode & **Michael Hughes,** Senior Principal Customer Success Manager, Veracode

13:00 Lunch & networking break

14:00 **Quantum computing and the future of security: HSBC's strategy to combat emerging threats**

Philip Intallura, Group Head of Quantum Technologies, HSBC

- Discover the fundamentals of quantum computing and why HSBC is investing in it for enhanced security and innovation
- Examine the potential risks quantum computing poses to existing cryptographic systems
- Explore HSBC's initiatives in cryptographic inventory, Post-Quantum Cryptography (PQC), and Quantum Key Distribution (QKD) to ensure quantum safety

14:20 **Stop chasing data: Control it where it lives**

Mohamed Djenane, Senior Director Sales Engineering MEA, Seclore

- In today's hyper-connected world, security teams are trapped in an endless chase – tracking sensitive data as it moves across networks, clouds, devices, and partners. This siloed approach leaves gaps, slows response, and drives up risk
- Discover how data-centric security eliminates the chase, unifies cyber and physical protection, and gives CISOs the control they need in a world beyond silos
- Learn how leading organisations are shifting from perimeter defence to persistent data protection – ensuring security travels with the file, wherever it goes, without disrupting business collaboration

14:40 **Rebooting the CISO role: Embracing agility and resilience**

Olivier Bussolini, Group CISO, Mashreq Bank

- Transitioning from traditional risk management to proactive business enabling
- Fostering a resilient, security-focused organisational culture
- Democratising decision-making to empower cross-functional collaboration
- Optimising security architecture for agility in an AI-driven era

15:00 **Education Seminars | Session 3**

Check Point Software Technologies	ManageEngine	ME InfoSec	Silent Push
Building the right cybersecurity architecture for a distributed world in the AI era **Sameer Basha,** Lead Sales Engineer & Evangelist, Check Point Software Technologies	**State of AI: How evolving intelligence in shaping cybersecurity** **Praneeth Vanteru,** Technical Consultant, ManageEngine	**Vulnerability remediation and patching – the real challenge** **Ara Awakian,** Chief Operations officer, ME InfoSec & **Minas Awakian,** Managing Director, ME InfoSec	**Pre-emptive cyber-defence: Finding adversary infrastructure before the attack** **Luke Angus,** VP EMEA, Silent Push & **Nick Roy,** Sales Engineer, Silent Push

15:40 Networking break

16:00 PANEL DISCUSSION **Securing future architectures**

Manit Sahib, Ethical Hacker, Cytadel & Former Head of Penetration Testing & Red Teaming, Bank of England (Moderator);
Rajesh Yadla, Head of Information Security, Leading Digital Bank;
Bader Zyoud, Head of Information Security Governance and Risk Management, Abu Dhabi Media Network;
Vijay Antony Velayutham, Principal Information Security Officer, UAE Ministry of Energy & Infrastructure;
Zaheer Mubarak Shaikh, CISO, Al Maryah Community Bank

- How can security teams design resilient architectures to integrate and leverage emerging technologies such as AI, quantum computing, and IoT?
- What role does AI play in developing proactive rather than reactive security strategies?
- What are the best practices for integrating AI without disrupting legacy systems and existing workflows?
- How can organisations implement zero-trust principles and adaptive access controls to secure ever-evolving environments driven by AI and edge computing?

16:30 **Ransomware 3.0: Weaponising AI for the next generation of ransomware attacks**

Manit Sahib, Ethical Hacker, Cytadel & Former Head of Penetration Testing & Red Teaming, Bank of England

- LIVE DEMO: Inside the first AI-powered ransomware attack – See how my custom Agentic Ransomware Gang can take down a network in under 8 minutes
- First-hand insights from real-world red team ops – from legacy tech and broken access controls to the critical lack of real-world security testing
- Why traditional security fails – compliance checklists and conventional tools don't stop modern ransomware
- What CISOs and security leaders must do now – real-world, field-tested steps to prove your controls work before attackers do it for you

16:50 Chair's closing remarks

17:00 Conference close

Education Seminars	
BeyondTrust **The impact of AI in identity security** **Theshan Mudaly,** Senior Solutions Engineer, BeyondTrust & **Saranraj Balaraman,** Partner Solutions Engineer, BeyondTrust	AI is everywhere – transforming the way we work, innovate, and solve problems. While this brings exciting opportunities, it also opens the door to new risks. Cybercriminals are now using AI to make their attacks smarter, faster, and harder to detect. By training AI systems on malware and other malicious tools, they are taking cyber-threats to an entirely new level. Join Theshan Mudaly, Senior Solutions Engineer at BeyondTrust, as he explores how AI is impacting identity security. Attendees will learn: • Breaking down how digital identities and privileges are now being targeted in new ways • Sharing how BeyondTrust's Modern PAM, combined with a least privilege strategy, can help organisations defend against these evolving AI-driven threats
Check Point Software Technologies **Building the right cybersecurity architecture for a distributed world in the AI era** **Sameer Basha,** Lead Sales Engineer & Evangelist, Check Point Software Technologies ME	Modern enterprises operate in highly complex, distributed networks, far from the ideal of cloud-only architecture. The shift to hybrid and distributed workspaces, accelerated by the AI era, has intensified cybersecurity challenges, leaving many architects uncertain about the right approach. Cybersecurity today must defend against diverse threats – cyber-warfare, ransomware, data theft, political conflicts, and vulnerabilities in edge devices – while protecting people, information, infrastructure, business operations, and reputation. Against this backdrop, organisations need guidance on building the right cybersecurity architecture, aligning strategy, controls, and monitoring evolving risks. We will use a practical example of home security analogy that audience can relate to derive the right cybersecurity architecture for a hybrid hyperconnected world. In essence, the presentation guides organisations toward a cybersecurity architecture that balances decentralisation with centralised oversight, leverages AI-powered threat prevention, continuous monitoring, and unified policies. Enriched with zero trust principles, this approach delivers resilient, adaptive security that mitigates evolving threats, aligns with business needs, and harnesses the opportunities and challenges of the AI era. Attendees will learn: • State of cybersecurity in a distributed AI-powered world • Embracing the right cybersecurity architecture • Open Garden and AI-powered threat prevention • Identity century and data-driven approach with zero trust philosophy
FileOrbis **Why data security falls apart without document security: The risk you can't afford to ignore** **Hammam Abunaser,** Sales Director – MEA, FileOrbis	In today's evolving digital landscape, organisations face increasing challenges from insider threats, data breaches, and ever-tightening compliance requirements. While investments in cybersecurity – such as firewalls, endpoint protection, and identity management – continue to grow, one area remains insufficiently addressed: unstructured data. Critical business information is often stored not in structured databases, but in documents – files that are routinely downloaded, shared, and transferred across various platforms, devices, and cloud environments. These actions frequently occur beyond the visibility and control of traditional security mechanisms. This speaking session will examine the strategic importance of incorporating document-level security into modern cybersecurity frameworks. It will highlight how organisations are implementing embedded access controls, encryption, and audit trails within files to maintain consistent protection, regardless of where the data resides. Attendees will learn: • Why document security is the missing layer in today's cybersecurity strategies • Why no amount of perimeter or device protection can make up for its absence • Exploring how forward-thinking organisations are embedding access controls, encryption, and auditability into the files themselves to ensure data remains protected wherever it goes

Education Seminars	
Infoblox **The overlooked risk: Why DNS is the new frontline in cyber-defence** **Ahmed Faragallah,** Solutions Architect, Infoblox & **Abdallah El Attar,** Senior Solutions Architect, Infoblox	'The Overlooked Risk: Why DNS is the New Frontline in Cyber Defence' highlights how the domain name system (DNS), the essential service that translates network names into IP addresses, has become a critical target and entry point for modern cyber-threats. Unprotected DNS can undermine the entire security stack. Implementing robust DNS security, including real-time monitoring and threat intelligence integration, elevates DNS from a basic resolver to an active line of early threat detection and prevention. Attendees will learn: • Understand the anatomy of zero-day DNS threats and how they bypass conventional security layers • Discover how to leverage AI-driven analytics to detect malicious domains in real time • Learn best practices for implementing proactive domain monitoring and threat intelligence
ManageEngine **State of AI: How Evolving intelligence in shaping cybersecurity** **Praneeth Vanteru,** Technical Consultant, ManageEngine	Discusses the evolution AI over the past decade and how the current models are gearing to address latest threats. Attendees will learn: • Evolution of AI over the years • How ManageEngine products incorporated various AI-related developments in our products • Our current focus areas related to AI • How we are planning to address cyber-threats using AI
ME InfoSec **Vulnerability remediation and patching – The real challenge** **Ara Antoun,** Chief Operations officer, MEInfoSec & **Minas Awakian,** Managing Director, MEInfoSec	Are you truly convinced that your 3rd-party application vulnerabilities are detected and remediated in a timely manner? Are you having challenges remediating vulnerabilities discovered in your VA reports (specifically configuration Vulnerabilities)? Does your VA report include a lot of false positives that repetitively appear in every monthly report? Are you truly convinced that your 3rd-party application vulnerabilities are detected and remediated in a timely manner? Join our session and share your thought and challenges with us and we will share with you our best practice. Attendees will learn: • A complete and comprehensive VA assessment – partial results have no value • A solution which is flexible enough to accommodate your infrastructure needs • An excellent support contract, to help you in a timely manner
Netskope **Securing data flow for the next wave of the AI era** **Kousain Raza,** Senior Solutions Engineer, Netskope & **Kamlesh Luhana,** Senior Solutions Engineer, Netskope	Sensitive data movement is often seen as a risk, but restricting it outright can create operational and security challenges. In an era of agentic AI and generative AI, organisations need security frameworks that protect data while ensuring agility. This session explores how modern security platforms enable secure data flow, adapt to diverse use cases, and prepare for the shift to an AI future. Attendees will learn: • How to enable data flows without introducing escalating security risks • How to choose the right secure access method for each use case • Why security must be adaptive to risk, user behaviour, and AI-driven interactions

Education Seminars	
Opentext **Re-imagine data privacy and protection in the AI era** **Khaled Saleh,** Regional Sales Manager – MEA Region, OpenText & **Salim Menikh,** Sales Manager, OpenText	As organisations embrace artificial intelligence to drive innovation, efficiency, and growth, the stakes for safeguarding sensitive information have never been higher. AI thrives on data, but the same data can become a vulnerability if not managed responsibly. A modern data privacy and protection framework must go beyond compliance – it should embed trust by design, balancing innovation with ethical responsibility. This means adopting advanced controls like intelligent data classification, AI-driven anomaly detection, encryption at scale, and privacy-preserving computation, all while aligning with evolving global regulations. In the AI era, protecting data is not just about security – it is about enabling sustainable trust, resilience, and long-term value creation.
Positive Technologies **Desert Dexter:** **The hidden cyber-threat in the Middle East** **Ilya Leonov,** Regional Director MENA, Positive Technologies	'Desert Dexter' is a social-media-driven malware campaign (since September 2024) across the MENA region that utilises fake news adverts linking to Files.fm/Telegram to deliver a modified AsyncRAT. Approximately 900 potential victims have been observed, with clues indicating a likely Libyan origin. Attendees will learn: • The playbook: fake-news ads → Files.fm/Telegram → RAR → BAT/JS → PowerShell → reflective loader injecting into aspnet_compiler.exe, plus persistence and Telegram-based data exfil • Capabilities to hunt: screenshots, system fingerprinting, checks for 2FA/crypto-wallet extensions/apps, and an offline keylogger • Practical takeaways: IoC lists (Files.fm/Telegram), an infrastructure map, targeted countries, and attribution hints (Arabic code comments, 'DEXTER' hostnames)
Sectona **From control to confidence: The new era of modern infrastructure access** **Javeria Malik,** Solution Engineer, Sectona & **Vishal Thakkar,** Director – Customer Success, Sectona	Today's enterprises operate across a vast and interconnected landscape – from on-premises infrastructure and cloud platforms and third-party networks. While this diversity offers unmatched flexibility, it also introduces complex privileged access challenges that traditional PAM solutions weren't built to address. Join Sectona for an exclusive session where we unveil our Modern Infrastructure Access approach – designed to secure every connection, everywhere, without compromising operational efficiency. Attendees will learn: • Achieving unified visibility and real-time control over privileged sessions • Enforcing least privilege and regulatory compliance seamlessly across diverse infrastructures • Securing access for internal teams, remote employees, and third-party users with minimal disruption • Eliminating blind spots and mitigating risks in hybrid and multi-cloud setups • Explore how Sectona brings diverse user personas together on a single, powerful platform

Education Seminars

Silent Push

Pre-emptive cyber-defence: Finding adversary infrastructure before the attack

Luke Angus, VP EMEA, Silent Push & **Nicholas Roy**, Sales Engineer, Silent Push

Cybersecurity teams often struggle with traditional threat intelligence as it can be largely reactive. Feeds can be overwhelming and difficult to operationalise. This leaves security teams playing catch up while adversaries are moving quickly. Silent Push takes a different approach by providing preemptive threat intelligence. Instead of using indicators of compromise (IOCs), the platform provides Indicators of Future Attack (IOFAs), which allows teams to identify attacker infrastructure earlier and before it is used in order to take action faster.

We will look at real-world examples where Silent Push uncovered malicious infrastructure tied to different campaigns and criminal networks. These case studies highlight how early detection helps take action sooner by detecting new infrastructure as early as possible. Finally, we'll explore practical use cases and how organisations can leverage preemptive threat intelligence into their existing security stack.

In this session, we will demonstrate how pre-emptive threat intelligence enhances detection and response, enabling security teams to act earlier in the threat lifecycle.

Attendees will learn:

- How to move from a reactive stance to a proactive defence posture, gaining strategies to stay ahead of evolving threats
- The challenges of traditional threat intelligence and why reactive methods fall short
- How Silent Push enables preemptive detection of adversary infrastructure
- Real-world campaigns and case studies showing Silent Push in action
- Practical use cases and how organisations can operationalise preemptive intel

Veracode

Is AI generated code secure?

Julian Totzek-Hallhuber, Senior Principal Solution Architect, Veracode & **Michael Hughes,** Senior Principal Customer Success Manager, Veracode

As generative AI becomes a mainstream tool for software development, one question is becoming increasingly urgent: Can we trust AI to write secure code? This session presents key findings from the 2025 GenAI Code Security Report, one of the most comprehensive evaluations to date of code security across over 100 large language models. Covering Java, Python, C#, and JavaScript, our research reveals troubling trends, including high failure rates on critical security tasks and no measurable improvement in security performance over time, even as models grow more powerful.

This session will help you navigate the real-world security implications of GenAI in your development workflow.

Attendees will learn:

- How often AI-generated code introduces vulnerabilities and in which languages
- What types of security issues are most common
- Why newer, bigger models aren't necessarily safer
- The hidden risks facing your software supply chain
- What developers and security teams must do to stay ahead