

Security

ADVISOR

MIDDLE EAST

ISACA
UAE Chapter

&
tahawultech.com
presents

INFOSEC & CYBERSECURITY

CONGRESS 2025

Securing the Intelligent Age

TRUST REIMAGINED IN INTELLIGENT AGE

SHAPING DIGITAL RESILIENCE WITH AI, ETHICS, AND CYBERSECURITY LEADERSHIP



1ST

IN THE REGION

PIONEERING CONVERSATIONAL AI AS A SERVICE

Our Industry Landscape



Retail



Healthcare



Banking



Education



Oil & Gas

Conversational AI Framework

NLP | Text-to-Speech | Generative AI | IDP

SCAN QR



LEARN MORE

OMNIX
Conversational AI





12

**ISACA UAE AND TAHAWULTECH
UNITE SECURITY LEADERS TO
CHART FUTURE OF TRUST IN
INTELLIGENT AGE**



18



82



86

6

Malaysia and UAE's Presight deepen digital ties with groundbreaking AI partnership

82

Roman Spitzbart, VP, Solutions Engineers at Dynatrace, shares insights on how the company is championing real-time observability, secure data governance and AI-powered automation.

18

GISEC Global 2025 powers resilience in an AI-driven world

86

The Critical Imperative of Healthcare Cybersecurity
Even life-saving technology can become life-threatening, as modern healthcare facilities are facing increasing attacks from cybercriminals.
By Nikola Kukoljac, Vice-President, Solution Architecture, Help AG.



ISACA
UAE Chapter

&
tahawultech.com
presents

INFOSEC & CYBERSECURITY CONGRESS 2025

Securing the Intelligent Age

📅 10th September 2025

📍 VOGO Abu Dhabi Golf Resort & Spa

🕒 09:00 AM onwards

SECURING THE INTELLIGENT AGE: BUILDING CYBER RESILIENCE FOR TOMORROW'S DIGITAL ENTERPRISES

The rise of intelligent technologies, AI-driven systems, and connected infrastructures has transformed cybersecurity into a boardroom priority. Security and risk leaders are now expected to be innovation champions—guiding organizations through complex digital environments while ensuring resilience, trust, and regulatory alignment.

The **Infosec & Cybersecurity Congress 2025**, hosted by **ISACA UAE Chapter** and **Tahawultech.com**, provides a powerful platform for meaningful discussions, real-world case studies, and forward-looking strategies. Industry leaders, CISOs, regulators, and innovators will converge to explore next-gen governance models, risk frameworks, and tech-driven defense mechanisms.

Join us on **10th September 2025** at **VOGO Abu Dhabi Golf Resort & Spa**,
and be part of the movement shaping the future of secure digital transformation.

GOLD SPONSOR

Delinea
Securing identities at every interaction

OFFICIAL PUBLICATIONS

cnme
computer news middle east

Reseller
MIDDLE EAST
THE VOICE OF THE CHANNEL

Security
MIDDLE EAST

HOSTED BY

tahawultech.com

#infosec&cybersecuritycongress2025 | #tahawultech | #isacauaechapter

EDITOR'S NOTE



Talk to us:

E-mail:

sandhya.dmello@
cpimediagroup.com

Sandhya DMello
Editor

UNITED FOR RESILIENCE: ISACA, GISEC LEAD CYBERSECURITY AGENDA

Cybersecurity is no longer just a technical function—it is a strategic priority, a national imperative, and a shared responsibility. This June, Security Advisor Middle East brings you unmatched coverage of two defining moments that have galvanized the region's cybersecurity narrative: the ISACA UAE Chapter's Infosec & Cybersecurity Congress 2025 and GISEC Global 2025, the Middle East and Africa's largest cybersecurity gathering.

At the ISACA Congress, experts, policymakers, and industry leaders converged to decode trust

in the Intelligent Age, tackling the rising influence of AI, quantum computing, and digital governance. The discussions were not just thought-provoking—they were blueprint-setting, marking a significant step toward reshaping the region's cyber risk frameworks.

Meanwhile, GISEC Global 2025 unveiled the next frontier in cyber resilience. With the launch of its first OT Security Conference, the event spotlighted industrial defense, AI-powered security, and the critical importance of collaboration across public and private sectors. From global thought leaders to regional changemakers, GISEC was a clarion call to innovate, integrate, and protect.

Complementing these coverages are sharp insights from cybersecurity front-runners

like Fortinet, SentinelOne, Huawei, Kaspersky, and Dynatrace, among others.

Strategic partnerships

such as Help AG's alliance with F5 and the UAE-Malaysia AI pact further illustrate the region's accelerating momentum toward a secure digital future.

This issue is a testament to how far we've come—and how united we must remain—as we secure what's next.

DEFINING TRUST IN DIGITAL ERA

EVENTS



FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by **CPI**

ADVERTISING
Group Publishing Director
Kausar Syed
kausar.syed@cpimediagroup.com

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

PRODUCTION AND DESIGN
Designer
Prajiith Payyapilly
prajiith.payyapilly@cpimediagroup.com

DIGITAL SERVICES
Web Developer
Adarsh Snehan
webmaster@cpimediagroup.com

Publication licensed by
Dubai Production City, DCCA
PO Box 13700
Dubai, UAE

Tel: +971 4 5682993

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

© Copyright 2025 CPI
All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

MALAYSIA AND UAE'S PRESIGHT DEEPEN DIGITAL TIES WITH GROUNDBREAKING AI PARTNERSHIP



Malaysia Madani Artificial Intelligence (MMAI Technologies SDN. BHD.), a wholly owned entity of the Malaysian Government, and Presight, a UAE-based leading global AI and big data analytics company, announced a landmark agreement set to accelerate Malaysia's digital transformation. This collaboration will harness advanced AI and sovereign cloud infrastructure to strengthen national security, enhance government efficiency, and drive data-powered governance.

The agreement, formally exchanged at the ASEAN-GCC Economic Forum 2025, marks a pivotal advancement in AI collaboration between the UAE and Malaysia, and is Presight's first major initiative in the South-east Asia region.

The exchange of agreements was conducted in the presence of His Excellency Anwar Ibrahim, Prime Minister of Malaysia, His Excellency Saifuddin Nasution Ismail, Minister of Home Affairs of Malaysia, and Peng Xiao, Group CEO of G42.

The partnership will see the two entities collaborate on a range of critical initiatives including the development of sovereign cloud infrastructure, AI solutions and applications for digital transformation across national safety, public security, and government efficiency.

"This partnership is uniquely strengthened by the UAE's proactive and pioneering efforts in artificial intelligence. Having embarked on its AI journey early, the UAE has made significant strides in both the practical application of AI technologies and the development of comprehensive governance frameworks. This rich experience, embodied by Presight, offers an invaluable foundation for Malaysia's own AI ambitions," said His Excellency Saifuddin Nasution Ismail, Minister of Home Affairs of Malaysia.

"The UAE's journey in AI, marked by its progressive policies and robust implementation, provides a powerful precedent. Through this partnership with Presight, Malaysia gains access to

world-class expertise that will propel our nation forward, aligning perfectly with our Malaysia Madani vision for a technologically advanced and digitally sovereign future.

"This collaboration not only boosts Malaysia's domestic resilience but also reinforces the strong bilateral relationship between Malaysia and the UAE, positioning both nations as pivotal contributors to the evolving global AI applications ecosystem."

Thomas Pramotedham, CEO of Presight, said: "This agreement exemplifies our commitment to using Applied AI to create tangible national impact. By partnering with MMAI, we are not only accelerating Malaysia's journey towards becoming a digitally advanced, AI-enabled economy, but also laying the foundation for long-term innovation, efficiency, and resilience across critical sectors.

"From secure data infrastructure to enhanced AI and analytics for key Malaysian agencies, we're pleased to

bring cutting-edge solutions that drive real progress. This collaboration reflects our shared belief that technology, when used responsibly and strategically, can be a catalyst for transformative change.

"We commend the leadership of Malaysia for their vision to enable economic growth through strategic investment in AI nation-building projects."

Advancing Shared National Priorities through AI

The Presight and MMAI agreement reinforces the strategic objectives of Malaysia's MADANI economic framework, launched by His Excellency Anwar Ibrahim in July 2023. The initiative seeks to elevate Malaysia's economic standing by promoting sustainable development,

fair wealth distribution, and robust investment in innovation. MMAI serves as the AI cornerstone in the nation's pursuit of these goals.

Today's announcement follows an MoU signed in Abu Dhabi on 13 January 2025, witnessed by His Highness Sheikh Khaled bin Mohamed Al Nahyan, Crown Prince of Abu Dhabi and Chairman of the Abu Dhabi Executive Council, and His Excellency Anwar Ibrahim, Prime Minister of Malaysia. The MoU outlined a shared commitment to invest in AI-driven capabilities designed to improve national safety, public security, and government efficiency.

This collaboration also builds on the momentum generated by the UAE-

Malaysia Comprehensive Economic Partnership Agreement (CEPA), confirmed in October 2024. Bilateral non-oil trade between the two countries reached US\$2.5 billion in the first half of 2024, a 7% year-on-year increase, highlighting the strength and growing depth of this relationship.

Presight Reinforces Thought Leadership on AI at ASEAN-GCC Forum

Alongside the exchange of agreements, CEO Thomas Pramotedham took part in a panel discussion at the ASEAN-GCC Economic Forum, titled: AI Impact Across Industries, where he shared insights on how AI is transforming sectors around the world and driving meaningful, real-world outcomes.

MIDDLE EASTERN ENTERPRISES TO ADVANCE CYBER RESILIENCE IN PUBLIC CLOUD WITH RUBRIK AND RACKSPACE TECHNOLOGY

Rubrik, a leading cyber resilience company, and Rackspace Technology (NASDAQ: RXT), a leading end-to-end hybrid cloud and AI solutions company, have announced Rackspace Cyber Recovery Service – a new managed service for customers operating in public cloud. By combining Rubrik's orchestrated data protection and cyber recovery solutions with Rackspace's DevOps principles and managed services, enterprises can simplify and accelerate recovery from ransomware attacks. Automated workflows deliver clean data and workloads through immutable backups, zero-trust architecture and Infrastructure as Code. With Rackspace Cyber Recovery Service, critical business workloads running in public clouds can be restored in hours, helping enterprises significantly strengthen their cyber resilience.

Why does this matter?

Recent deals demonstrate that Middle Eastern investment in cloud, AI and data centre projects are ramping up. These local initiatives are in pursuit

of regional goals, such as the Saudi 2030 Vision, diversifying the country economically, socially and culturally. Organisations in the Middle East are therefore digitalising at scale. Businesses that run key workloads in

public clouds face growing challenges when responding to cyber attacks – from limited visibility and inconsistent backup policies to slow recovery times and lack of automation to rebuild at scale. At the same time, IT leaders are grappling with



increasingly complex and distributed cloud environments, making it difficult to maintain consistency, ensure visibility and execute reliable recovery. Recently, Rubrik Zero Labs revealed that 90% of EMEA IT and security executives reported cyber attacks in the last year. In the event of major disruptions – such as ransomware attacks – many enterprises struggle to restore critical workloads quickly due to fragmented tooling, manual processes, untrusted data and inadequate automation.

“Enterprises can no longer rely on traditional recovery methods in a cloud-first, threat-intensified world,” said DK Sinha, President for Public Cloud at Rackspace Technology. “To ensure recoverability in the public cloud, they must adopt a new approach that leverages cloud native tools, modern DevOps methodologies and trusted expertise. Through our partnership with Rubrik, Rackspace Cyber Recovery Service sets a new standard for cyber resilience of public cloud workloads.”

Rackspace Cyber Recovery Service Extends Fast and Confident Cyber Resilience to Public Cloud

Rackspace Cyber Recovery Service applies Infrastructure as Code and platform engineering principles to

cyber recovery, enabling restoration of critical workloads across multi-cloud environments. The journey begins with a professional services-led transformation, where Rackspace experts modernise recovery architectures and codify resilient workflows tailored to each environment. These capabilities are then transitioned into a ‘Day 2’ fully managed service, ensuring continuous validation, optimisation and operational readiness. By orchestrating Recovery as Code, the solution delivers rapid, repeatable and auditable workflows aligned with modern DevOps practices. Paired with Rubrik’s immutable architecture and AI-driven threat detection and containment, it ensures clean data recovery into secure landing zones with minimal operational disruption.

“Amidst the evolving complexities of multiple cloud environments, proactive cyber resilience is not a luxury but a necessity. Together, Rackspace and Rubrik offer a differentiated, engineering-led approach to cyber resilience,” said Ghasal Asif, Vice President of Global Channels and Alliances at Rubrik. “Specifically designed for complex, distributed cloud environments, our companies are at the forefront of safeguarding organisations against the rising tide of ransomware

attacks in the realm of cloud and SaaS platforms.”

Rackspace Cyber Recovery Service provides enterprises running public cloud workloads with:

- **Proactive Protection:** Continuous anomaly detection and threat monitoring to identify and resolve potential issues before they impact backups or recovery capabilities
- **Expert Management:** Optimal backup configuration, policy and lifecycle management
- **Cloud Management:** Infrastructure management services to ensure your applications are managed efficiently in the cloud while infrastructure and data restoration procedures are tested for recovery during incidents or disasters
- **Improved Compliance:** The ability to support data retention policies and regulatory requirements with consistent management and detailed reporting
- **Advisory & Professional Services:** Strategic guidance and implementation of Rubrik-powered cyber recovery solutions – including RTO/RPO planning, regulatory alignment and deployment of automated Infrastructure as Code workflows into secure landing zones

BEWARE OF FAKES: SCAMMERS USE LABUBU DOLL HYPE ON MULTILINGUAL SCAM WEBSITES

The skyrocketing popularity of Labubu dolls has triggered a wave of scam websites targeting enthusiastic collectors worldwide, with cybercriminals deploying fake online shops in multiple languages to steal payment details. Kaspersky detected hundreds of fraudulent platforms, often posing as legitimate retailers, that entice fans with fake offers on Labubu dolls to harvest sensitive financial information from unsuspecting buyers.

Labubu dolls, quirky plush collectibles

designed by Hong Kong artist Kasing Lung and sold by Pop Mart stores in “blind boxes,” have captivated global audiences. Buyers do not know which specific doll or design they’ll get until they open it. This element of surprise, combined with the chance of getting rare or limited-edition figures, fuels the excitement and collectible frenzy.

Since April 2024, the hype multiplied, fuelled by high-profile celebrity endorsements, leading to resale prices for rare dolls reaching \$3,000 and above.

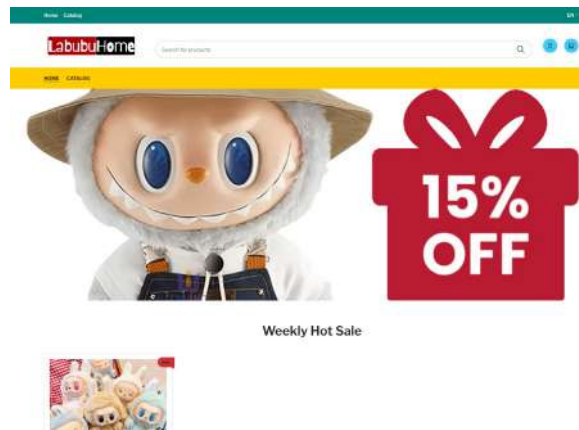
This has created a fertile ground for scammers, who exploit the urgency and excitement surrounding these coveted toys.

A scam website claims to sell “Labubu originals” and describes the story behind the creation of Labubu dolls. Multiple figures are offered at “special prices” ranging from \$30 to \$79.99

Cybercriminals create counterfeit websites in multiple languages to deceive buyers in different regions. These fake shops often mimic the

branding of trusted retailers, offering discounts or “exclusive editions” of dolls to lure victims into entering bank card details or other personal information. Pop Mart is the official retailer and creator of Labubu dolls, and scammers mimic its appearance to trick buyers into thinking they are purchasing authentic products.

“Scammers are leveraging the Labubu hype with scam sites and urgent calls-to-action that prey on



fans’ eagerness to snag rare dolls. These fraudulent platforms are now appearing in multiple languages, which broadens their reach. Fans are strongly advised to purchase Labubu dolls only from verified retailers like Pop Mart’s official channels after double-checking the website’s URL for authenticity, and avoid interacting with websites that seem suspicious,” said Olga Altukhova, Senior Web Content Analyst at Kaspersky.

SOPHOS UPDATES SOPHOS FIREWALL SOFTWARE TO ENHANCE PROTECTION AND INCIDENT RESPONSE CAPABILITIES

Sophos, a global leader of innovative security solutions for defeating cyberattacks, announced an update to its Sophos Firewall, now including Sophos NDR Essential, which is free for all customers with an XStream Protection license for Sophos Firewall.

With this integration, Sophos Firewall leverages two dedicated artificial intelligence engines to detect malware communications and communications using algorithmically generated domain names. This new feature, stemming from the Sophos Network Detection and Response probe, aims to identify malware communications even when they are previously unknown or not yet indexed. It complements the Active Threat Response capabilities already implemented in Sophos firewalls.

Chris McCormack, Senior Product Marketing Manager at Sophos, said: “NDR traffic analysis requires substantial processing power. That’s why we’ve adopted a new approach by deploying an NDR solution in Sophos Cloud to offload the heaviest tasks from the firewall.”

Sophos Connect now integrates EntraID for SSO.

This new feature of the VPN client bundled with Sophos Firewall enhances both security and user experience for



Chris McCormack, Senior Product Marketing Manager at Sophos.

SSL and IPSEC VPN connections. It is now possible to use EntraID (Azure AD) to authenticate users and implement multi-factor authentication for Sophos Connect and access to the user portal hosted by the firewall.

Other VPN-related improvements include:

- Improved user interface and usability: Connection types have been renamed from “site-to-site” to “policy-based”, and tunnel interfaces have been renamed “route-based” to make them more intuitive.
- Dynamic validation of the IP address pool allocated to VPN connections (SSL

VPN, IPsec, L2TP, and PPTP) to better resolve potential IP address conflicts.

- Strict profile enforcement: In IPsec profiles, default values are now excluded to ensure algorithm synchronization, thereby eliminating possible fragmentation of session negotiation packets that could otherwise prevent site-to-site VPN tunnels from being established.
- Route-based VPN and SD-RED scalability: The system now supports up to 3,000 simultaneously established tunnels. Sophos Firewall solutions can now handle up to 1,000 SD-RED site-to-site tunnels and up to 650 concurrent SD-RED devices.

Additional management improvements include:

- More flexible DHCP Prefix Delegation (IPv6 DHCP-PD): Now supports /48 to /64 prefixes, improving compatibility with certain internet service providers.
- Router Advertisement (RA) and DHCPv6 server: Now enabled by default.
- Resizable table columns: The web admin interface continues to adapt to ultra-wide screens, and many configuration pages now allow column resizing as needed.
- Enhanced object search functionality: The search field in the SD-WAN routing

configuration screen now supports more criteria (route name, ID, objects, object values such as IP addresses and domains, among others). Local ACL rules now also support object name and value searches, including content-based searches.

- **Default configuration changes:** Default firewall rules and rule groups previously created during new firewall setups have been removed. Only the default network rule and MTA rules are now provided in the initial configuration.

The default firewall rule group and the default gateway probe for custom gateways are both now set to "None" by default.

Secure by Design

Sophos continues to enhance the intrinsic design of its firewalls. The secure-by-design approach includes containerization of specific features and integrity checks on critical operating system files using mathematical checksums. Any checksum

mismatch triggers a potential compromise alert, allowing monitoring teams to proactively identify possible security incidents affecting the firewall OS integrity. Incident response and development teams are then able to react swiftly to critical incidents.

Availability

Customers can now manually download and deploy this update on any Sophos Firewall equipped with a valid license.

HELP AG, PARTNERS WITH F5 TO LAUNCH MANAGED APP AND API PROTECTION

Help AG, the cybersecurity

arm of e& enterprise, has inked a strategic partnership agreement to be the first Managed Services Provider (MSP) partner for F5 in the Middle East region.

Building on a long-standing partnership with F5, Help AG has launched its next-generation Managed App and API Protection Service based on the F5 Distributed Cloud Platform. This is an always-on, cloud-delivered managed service for the AI era, designed to secure modern digital infrastructure across public, private, edge, and hybrid cloud environments.

Today's threat landscape is more complex, with malicious actors being able to access a broader attack surface as enterprises rapidly shift towards API-driven architectures, edge computing, and cloud-native applications. From automated bot attacks and API abuse to sophisticated Distributed Denial of Service (DDoS) attempts, the pressure on security teams has never been greater. The problem is exacerbated by the fact that many enterprises lack the knowledge and tools to protect themselves against these types of attacks

Help AG's Managed App and Application Protection service directly addresses these evolving challenges by providing multi-layered protection



The Help AG and F5 teams at the signing ceremony. Stephan Berner, CEO, Help AG (fifth from left), described the partnership as a "strategic leap forward for enterprise security".

as a managed, Software-as-a-Service (SaaS) offering. Backed by F5's globally recognized F5 Distributed Cloud Services and operated 24x7 by Help AG's expert SOC team, the new service enables clients to simplify operations, ensure compliance, and respond to threats in real time. Leveraging Help AG's local expertise and managed service leadership, businesses can now deploy resilient, compliant, and cost-efficient application protection.

Stephan Berner, Chief Executive Officer of Help AG, said: "This is a strategic leap forward for enterprise security. Our collaboration with F5 reflects our shared vision of securing every application, API, and digital interaction, at scale. With this new service, we are providing regional organizations with enterprise-grade security that is proactive, cost-effective, and built for the cloud-first era."

The solution provides unified protection that includes Web Application Firewall (WAF), advanced bot mitigation, API discovery and security, plus DDoS defense; all accessible through a centralized SaaS-based management console that ensures full visibility and control. Clients benefit from flexible deployment models across regional and customer edge locations, hybrid setups, and full support and continuous

tuning by Help AG's expert teams.

Mustapha Hlil, Director of Channel Sales for the Middle East, Türkiye and Africa at F5, commented: "As cyber threats become more sophisticated and widespread, the need for always-on, adaptable security has become mission-critical. Help AG's security expertise, managed services leadership and state-of-the-art SOC with 24x7 support – combined with the F5 Distributed Cloud platform – provides a powerful solution for customers navigating complex digital transformation journeys. It will also significantly help enterprises lacking the expertise to deploy and manage security solutions."

The launch marks a new chapter in the Help AG and F5 partnership, further strengthening their joint commitment to securing the region's digital future and helping organizations build trust in every digital interaction.



CHANNEL LEADERSHIP FORUM & AWARDS 2025

CELEBRATING EXCELLENCE. SHAPING
THE FUTURE OF CHANNEL LEADERSHIP



22ND JULY 2025



RAFFLES DUBAI



9:00 AM TO 1:30 PM

Recognising Vision. Celebrating Excellence. Shaping the Future of the Channel.

The Channel Leadership Forum & Awards 2025 is a defining annual celebration of innovation, transformation, and success within the regional channel ecosystem. This prestigious event brings together the most influential figures from across the partner, vendor, and distributor landscape to honour standout achievements and forward-thinking leadership.

Now in its latest edition, the event highlights those who continue to push the boundaries—driving digital acceleration, enhancing customer value, and building next-generation partner models.

From leadership in AI and cloud to excellence in service delivery and partner engagement, this forum provides a platform to connect ideas, celebrate growth, and set the stage for the channel's future.

Join us for an inspiring day of insights, recognition, and connection.

OFFICIAL PUBLICATIONS



HOSTED BY



tahawultech.com

#ChannelLeaders25 | #tahawultech



ISACA UAE AND TAHAWULTECH UNITE SECURITY LEADERS TO CHART THE FUTURE OF TRUST IN THE INTELLIGENT AGE

INFOSEC & CYBERSECURITY CONGRESS 2025 DELVES INTO THE EVOLVING DIGITAL THREATSCAPE, AI PARADOXES, AND BUILDING RESILIENCE AMID GLOBAL UNCERTAINTY.

The 2025 edition of Infosec & Cybersecurity Congress, hosted jointly by ISACA UAE Chapter and tahawultech, brought the region's cybersecurity community together under the powerful theme: 'Securing the Intelligent Age'. In an era where AI, quantum computing, and blockchain are rapidly redefining digital ecosystems, the Congress provided actionable insights for industry leaders, CISOs, and security professionals to navigate today's complex

and evolving threat landscape.

Opening the day, Sandhya D'Mello, Editor, CPI Media Group, welcomed attendees and set the tone for the event, underscoring the need for collaborative innovation to stay ahead of cyber adversaries. This was followed by opening remarks from Dr. Alok Tuteja, CGEIT, CRISC, Ex-President, ISACA UAE Chapter, who addressed the imperative of Digital Trust — emphasising its critical role in safeguarding an interconnected future.

The rise of AI-driven systems and automated decision-making is accelerating across industries, bringing profound opportunities but also widening a trust deficit. Growing concerns around data privacy, algorithmic bias, transparency, and accountability are creating gaps between emerging technologies and public trust. To bridge these divides, organisations must embrace ethical frameworks, foster AI explainability, and champion responsible innovation that inspires confidence



among users, partners, and regulators.

The first panel discussion, titled 'Navigating the trust deficit in the Intelligent Age', explored these challenges and solutions in depth. Panelists Taskeen Khan, Aditya Kaushik (ZMI Holdings), Padam Sundar Kafle (Aster Digital Health), and Jayesh Nandan (Mediclinic Middle East)

offered compelling perspectives on embedding trust at the core of digital transformation.

A major highlight was the keynote by Gopan Sivasankaran, General Manager, META, Secureworks (a Sophos company), titled 'Think like Attackers – The Shift beyond EDR'. He urged organisations to adopt an attacker's mindset, moving

beyond traditional endpoint detection and response to a more proactive, threat-informed defense posture.

AI's double edge in the perfect storm – Navigating security paradoxes amidst converging global risk was the focus of the next panel. Speakers Dhiraj Sasidharan, Oma Martins – Okonkwo (IHS Towers), and Annu Chouraria





addressed how AI simultaneously serves as both an enabler of stronger security and a source of new threat vectors. The discussion explored paradoxes such as AI-driven automation improving threat detection while also expanding attack surfaces, the challenges of managing AI-generated misinformation, and the risks of adversarial AI. The panel emphasised the need for dynamic governance, cross-functional collaboration, and continuous risk monitoring to harness AI's benefits while mitigating emerging risks.

Building resilience — through strategy, culture, and digital trust — has never been more critical amid today's volatile threat environment. Cyberattacks are no longer isolated technical events; they impact business continuity, brand reputation, customer confidence, and even national security. A resilient organisation must embed cybersecurity into its strategic planning, foster a culture of security awareness across all levels, and integrate digital trust as a core principle in its operations. This holistic approach ensures organisations are not merely reactive but can anticipate, withstand, and recover from evolving digital threats.

In an age marked by uncertainty and

Cybersecurity Visionary Leader of the Year

- **H.E. Dr. Mohamed Al Kuwaiti**
UAE Cyber Security Council (CSC)

CISO Infosec & Cyber Risk Leadership Awards

- **Dhiraj Sasidharan**
Emirates NBD
- **Kausar Mukeri**
GEMS Education
- **Sajjad Ahmad**
DP World
- **Anand Nataraj**
Emaar
- **Oma Martins-Okonkwo**
IHS Towers
- **Ahmed Nabil Mahmoud**
Abu Dhabi Islamic Bank (ADIB)
- **Ram Soni**
Mashreq
- **Ahmed AlZarouni**
Investment Corporation of Dubai
- **Sunil Nair**
Majid Al Futtaim Retail LLC

Strategic Leadership In Cyber Community Development

- **Kapil Matta**

escalating digital risks, the final panel on 'Building resilience – Strategy, culture, and digital trust' brought together Faisal Khan (Dubai World Trade Centre), Zahid Altaf (Majid Al Futtaim Holding LLC), Abraham Rabind Parbhunath (Federal Authority for Nuclear Regulation), and Muhammad Musa Mazhar (Liva Group). The discussion centred on aligning cyber resilience with organisational culture, leadership, and long-term trust frameworks.

The event also featured a compelling fireside chat between Harriet de Morton, SASE Sales Manager for Middle East & Africa, HPE Aruba Networking, and Shijeesh Sahadevan, WAN & Security Transformation Expert, HPE Aruba Networking. The session explored SASE (Secure Access Service Edge) and how organisations can adopt secure networking models fit for the hybrid era.

Infosec & Cybersecurity Congress 2025 affirmed that while technology is evolving at breakneck speed, the fundamental pillars of trust, resilience, and collaboration remain the foundation of a secure digital future.

The awards ceremony hosted towards the close of the event revealed the winner of CISO Infosec & Cyber Risk Leadership Award. 🏆

Secure Your **Digital Future**

Simple. Secure. Resilient.



**Secure Your Enterprise IT Footprint
For A Safer Digital Journey**

www.raqmiyat.com

UAE | KSA | INDIA

Security

ADVISOR

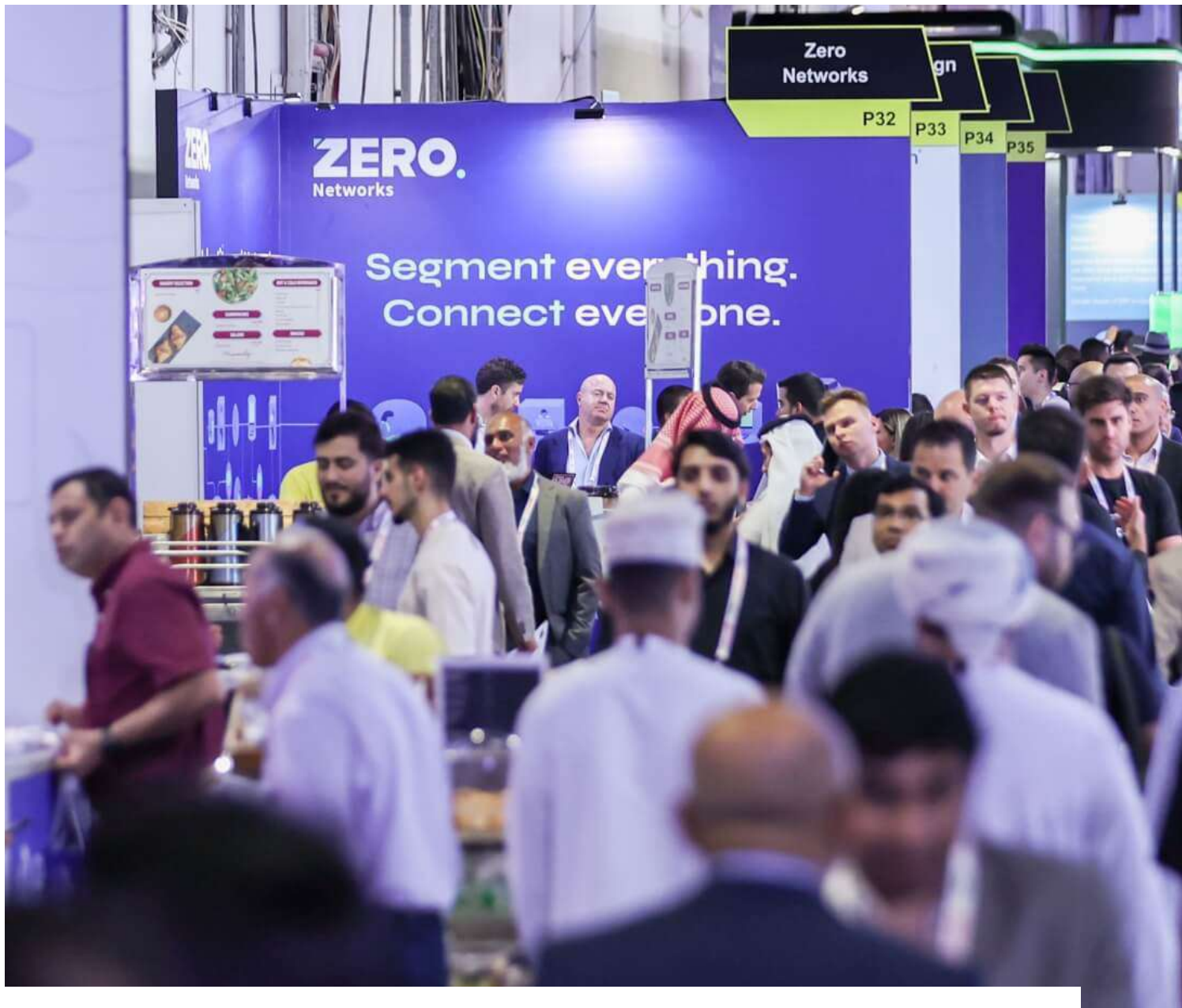
SPECIAL REPORT

MIDDLE EAST



THE FUTURE IS SECURE





GISEC GLOBAL 2025 POWERS RESILIENCE IN AN AI-DRIVEN WORLD

MIDDLE EAST & AFRICA'S LARGEST CYBERSECURITY EVENT
LAUNCHES OT SECURITY CONFERENCE TO COMBAT SURGING
INDUSTRIAL THREATS



By Sandhya D'Mello

GISEC Global, Middle East & Africa's largest and most impactful cybersecurity event, hosted its 14th edition at Dubai World Trade

Centre from May 6 to May 8, 2025, under the overarching theme of 'Securing an AI-Powered Future'. Organised by Dubai World Trade Centre and supported by Dubai Electronic Security Center (DESC), UAE Ministry of Interior, and Dubai Police.

Following the success of 2024, the super-connector event for the region's cybersecurity industry brought together over 25,000 attendees, 750 exhibiting brands and 350-plus speakers hailing from over 160 countries. Cyber threats are growing rapidly in both frequency and sophistication, creating an urgent need for advanced cybersecurity solutions. Businesses, individuals, and governments face unprecedented risks from cyberattacks as technology becomes increasingly intertwined with everyday life.

GISEC Global 2025 provided a vital forum to explore critical topics such as data privacy, securing the networks that power modern innovations, and crafting effective strategies to confront the constantly evolving digital threat landscape.

H.E. Dr. Mohamed Al-Kuwaiti, Head of Cybersecurity, UAE Government, said: "GISEC Global arrives at a pivotal moment when cyber threats are growing in both prevalence and sophistication. The need for robust cybersecurity measures has become essential for businesses, individuals, and governments alike, since everyone remains at risk of cyberattacks. Therefore, we are eager to explore key topics such as: Data privacy, securing the networks that drive these innovations, and developing strategies to counter evolving digital threats."

Similarly, H.E. Amer Sharaf, CEO of Cyber Security Systems and Services Sector at the Dubai Electronic Security Center (DESC) plays a crucial role in ensuring the city's digital resilience. Events like GISEC are essential platforms for fostering collaboration, knowledge exchange, and cybersecurity innovation. Looking ahead, DESC remains committed to leveraging emerging technologies, AI-driven security solutions, and strategic partnerships to build a secure and interconnected digital ecosystem for Dubai's future."

GISEC Global 2025 launched OT Security Conference as cyberattacks

on critical infrastructure surge 49%.

The new dedicated track at Middle East and Africa's largest cybersecurity event tackled AI-driven industrial threats, Zero Trust adoption, and the \$44.9B OT security boom.

The OT-focused conference at GISEC Global tackled evolving risks, system vulnerabilities and strategies for securing critical infrastructure. Other important considerations included AI in ICS/OT Security, Quantum Computing Threat, Protecting ICS and SCADA Systems & Digital Supply Chains in the presence of top CISOs, CIOs, OT security heads and policy-makers to fortify SCADA, ICS and digital supply chains.

The global OT security market is projected to double to \$44.9 billion by 2029 (Markets and Markets). According to research by IBM, the average cost of cyberattacks on organisations in the Middle East is \$8.75 million, nearly double the global average.

Why OT Security? Why Now?

OT security encompasses advanced cybersecurity protocols designed to ensure the integrity, availability and safety of industrial control systems. Robust OT security is essential for maintaining continuity across the oil & gas, manufacturing, energy, transport and utility sectors as critical infrastructure faces escalating cyber threats,

In late 2024, ransomware groups accelerated attacks on industrial sectors, with manufacturing, transportation and ICS operations prime targets. Only aggressive defence, intelligence sharing and cross-sector collaboration will safeguard critical infrastructure into 2025 and beyond.

The audience heard from experts on the need for modern OT protection which delved into precision AI, leveraging machine learning, deep learning and large language models.

Discussing cybersecurity threats in the maritime industry, where ships can hold up to 10,000 passengers, are driven

autonomously and each country has their own set of AI regulations, Simone Fortin, Global CISO Cruise Division at MSC Cruise Division, called for streamlined regulations that can be applied to all countries around the world.

He said: "For an industry like maritime, which is regulated by the UN, it is hard to interpret how to prevent AI threats for something critical like managing a ship. The UN gives the policy a broader scale, but then everything is regulated by bilateral agreements between the states and the regulators, and implemented by companies; but then, everything is defined by the fact that you could be in international waters. And ships can be owned by one entity, managed by another while sailing under a separate flag."

Bridging the gap between AI-powered cyber defence and critical infrastructure resilience, the OT Security Track also put the spotlight the escalating IoT/IIoT threats in the oil & gas sector, featuring frontline insights from global CISOs defending the world's most targeted industries.

Amal Krishna, Executive Director & CISO, ONGC, said: "To combat the surge in OT cyberattacks, businesses must prioritise asset visibility, network segmentation and secure remote access – but equally critical is breaking down silos between IT, OT and engineering teams. Cyber resilience in critical infrastructure isn't just about technology, it's about collaboration, continuous monitoring and a security-first culture."

Albert Vartic, Upstream OT Cybersecurity Officer, OMV Petrom, added: "Over the next five years, OT cybersecurity in the Middle East's critical infrastructure will see significant evolution. The region's rapid digitalisation has expanded the attack surface, making industrial systems more vulnerable – proactive measures like IEC 62443 adoption and cross-team collaboration will be essential to safeguard operational resilience."

Protect and plan against digital attacks

Exhibitors Ayman Al Issa (CPX) and Mohammed Mousa (CyberKnight) dissected the 49% surge in OT attacks, offering actionable defences for the energy, healthcare and manufacturing sectors.

Mousa, OT/xIoT Consultant at CyberKnight, warned that legacy OT systems weren't built for today's threats.

He explained: "The escalation in intrusions is a consequence of accelerated digital transformation in industrial sectors. As organisations integrate IT and OT environments to improve efficiency and support the business, they inadvertently expand the threat surface.



Furthermore, legacy systems remain in operation far beyond their intended lifespan and often lack native security controls.

"Meanwhile, increased reliance on remote access, third-party integrations, and limited OT-specific cybersecurity governance heightens exposure. Simply put, organisations are moving faster than their security strategies are evolving."

For businesses and governments to stay ahead of cyber criminals, Al Issa, Director – OT Cybersecurity at CPX, emphasised the importance of undertaking risk and threat assessments to understand what assets are at risk and how potential attackers might target them, sooner rather than later.

He said: "In today's fast-shifting business landscape, organisations need to focus on identifying their most critical assets – those that are at the highest risk and that they care about the most, rather than trying to protect everything or plan for recovery across the entire business. As such, organisations should conduct in-depth threat and risk assessments specifically considering the unique characteristics of industrial control systems (ICS), including their physical consequences.



**H.E. Dr. Mohamed Al-Kuwaiti
 Head of Cybersecurity, UAE Government**



"This involves mapping out interdependence, potential attack vectors and consequences of downtime. Using threat intelligence and aligning with frameworks like CIS ICS Controls can help organisations monitor suspicious activity, manage vulnerabilities and create tailored incident response plans.

"Once this is clear, more targeted and practical defence measures can be put in place and continuously tested, using threat intelligence to stay ahead of evolving threats. Risk assessments should be continuous, evolving with technological changes and emerging threats and should be validated through regular penetration testing."

Amr Elsayed, Regional OT/ICS Cybersecurity Specialist at CyberKnight,

agrees, saying technology, collaboration and workforce training should be key priorities for businesses.

He said: "To enhance OT security resilience against rising cyber threats, businesses should adopt a Zero Trust approach, enforcing least-privilege access and micro-segmentation to limit breach impact. Advanced real-time monitoring and threat intelligence sharing (ISACs, public-private partnerships) are critical for proactive defences.

"Additionally, maintaining accurate OT asset inventories, conducting OT-specific incident response drills and implementing risk-based vulnerability management (compensating controls, tailored patching) will strengthen security postures. Finally, OT-focused employee training ensures a security-aware workforce.

"By prioritising these measures – spanning technology, collaboration and workforce readiness – organisations can safeguard critical infrastructure, mitigate disruptions and build long-term cyber resilience in OT environments."

Drafting the legislation playbook

With Middle East nations rapidly adopting digitisation into their day-to-day practices, the region is becoming a target for cyberattacks. However, the experts expect a number of measures to be put in place to protect cybersecurity infrastructure, and GISEC 2025 could be where policymakers and tech giants will draft the playbook.

Al Issa added: "Over the next five years, we can expect a major shift toward structured, regulation-driven cybersecurity approaches. AI-driven OT threat detection, the widespread adoption of Zero Trust principles and deeper integration of compliance frameworks will define the regional OT cybersecurity landscape. Stricter regulatory frameworks and compliance mandates region-wide will push for better security practices. 📌

THE NEED FOR ROBUST CYBERSECURITY MEASURES HAS BECOME ESSENTIAL FOR BUSINESSES, INDIVIDUALS, AND GOVERNMENTS ALIKE, SINCE EVERYONE REMAINS AT RISK OF CYBERATTACKS.
H.E. DR. MOHAMED AL-KUWAITI, HEAD OF CYBERSECURITY, UAE GOVERNMENT

SANS INSTITUTE ON AI SECURITY: PREPARING FOR EMERGING THREATS IN 2025

ROB LEE, CHIEF OF RESEARCH AND HEAD OF FACULTY AT SANS INSTITUTE, DISCUSSES THE ACCELERATING AI-DRIVEN THREATS ORGANISATIONS WILL FACE AND THE VITAL SECURITY CONTROLS NEEDED TO MITIGATE RISKS IN 2025.

The rapid evolution of AI technologies is presenting organisations with an increasing set of cybersecurity challenges.

Rob Lee, Chief of Research and Head of Faculty at SANS Institute, highlights the emerging AI-driven threats and the importance of implementing robust security controls to protect against them. Lee explores the role of reasoning agents in cyberattacks, the need for proactive security measures, and SANS Institute's efforts to help organisations navigate the fast-paced AI security landscape in this interview with Sandhya D'Mello, Technology Editor, CPI Media Group.

With AI technologies rapidly advancing, what emerging threats do you anticipate organisations will face in the coming years, particularly as we move towards 2025?

The biggest threat I believe, in artificial intelligence that is being developed by adversaries, is reasoning agents. The capabilities would allow for automatic exploitation, moving through the kill chain from initial penetration to a

spear-phishing attack or a zero-day exploit, laterally moving and doing privilege escalation, identifying targets, and either implanting or committing skilled data. The steps used to take a human operator weeks, maybe months to accomplish, but reasoning agents are theoretical and already proven through MIT research to be 45 times faster than humans in performing the same operations. This means we're talking timeframes in seconds, rather than weeks or months.

Why is it crucial for enterprises to implement AI security controls, and what are the key risks that should be addressed to ensure secure AI adoption?

Many organisations feel that if they do not lean forward and adopt AI technologies, they will be left behind, as new models are released almost weekly with higher performance and lower cost. The challenge lies in implementing them quickly while ensuring the model's security. Executives are grappling with whether the models they are adopting could potentially disrupt their networks. It's important for businesses to assess and audit AI models swiftly to determine their security posture. The risk lies in not having appropriate guardrails for these models, which could lead to vulnerabilities. Ensuring these models are secure before implementation is a double-edged sword and a key area of focus.

REASONING AGENTS ARE ALREADY PROVEN TO BE 45 TIMES FASTER THAN HUMANS IN PERFORMING CYBER OPERATIONS, REDUCING THE TIMEFRAMES FROM WEEKS OR MONTHS TO MERE SECONDS."

ROB LEE, CHIEF OF RESEARCH AND HEAD OF FACULTY, SANS INSTITUTE



Rob Lee
Chief of Research and Head
of Faculty, SANS Institute.

Could you share insights into how organisations can effectively integrate AI into their systems using a risk-based approach, ensuring both security and operational effectiveness?

Organisations often make excuses, saying they cannot implement AI securely at the moment. However, SANS has released its first AI Critical Controls Guide, which outlines the top six controls executives should evaluate before implementing AI models. This guide was launched in April and is

available on the SANS website. While many organisations feel they don't know how to proceed, SANS is providing the critical questions they should ask before deploying AI systems, helping to fill the gap in knowledge and ensure secure integration.

How does SANS Institute's participation at JITEC align with your mission to help organisations secure AI technologies?

GISEC and similar events are essential for focusing the industry on what is

currently available in AI security. SANS has released the AI Critical Controls Guide and continues to lead efforts to educate the community on these issues. Our participation at such events helps raise awareness and promotes industry collaboration, allowing us to share our resources and encourage expert feedback. By engaging with the community, SANS is committed to providing valuable guidance and resources for businesses seeking to adopt AI securely. 🔑

FORTINET LEADS THE CHARGE IN AI-ENABLED SECURITY AGAINST EVOLVING CYBER THREATS.

TONY ZABANEH, DIRECTOR OF SYSTEMS ENGINEERING, SOUTH MIDDLE EAST, FORTINET, SHARES INSIGHTS WITH SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP, ON FORTINET'S AI-DRIVEN SOLUTIONS, SASE, ZERO TRUST ACCESS, AND STRATEGIES TO COMBAT MACHINE-POWERED CYBER THREATS IN THE MIDDLE EAST.

Fortinet is a leading force in cybersecurity, driving innovation by strategically integrating Artificial Intelligence to strengthen security frameworks. This AI integration leads to faster response times and improved operational efficiency, fundamentally reshaping organisations' security. The company consistently provides key insights into how AI-enabled security is revolutionising the cybersecurity landscape, particularly within the Middle East. Fortinet takes a forward-thinking and proactive approach, embedding AI technologies within its comprehensive range of security solutions, enabling businesses in the Middle East to stay ahead of increasingly sophisticated cybercriminal tactics.

Zabaneh shares that Fortinet is not just adapting to the changing threat landscape; it is actively building and defining the future of cybersecurity in the region. This commitment positions Fortinet as a key player in securing digital assets and infrastructure against the rising tide of cyber threats, ensuring a more resilient and protected digital environment.

What are some of the key security solutions Fortinet is showcasing this year?

This year, the focus is on Secure Access, known in the industry as SASE (Secure Access Service Edge), and Zero Trust Access. Additionally, significant emphasis is being placed on AI-enabled security, with live demos running in real customer use cases. These technologies are designed to address some of the biggest cyber security challenges businesses face today.

Cyber threats in the Middle East have been evolving rapidly. What are the most critical risks businesses are dealing with?

The biggest emerging threats are machine-powered attacks. Over the past few years, there's been an increase in sophisticated, AI-driven attacks. These attacks are faster, larger-scale, and more difficult to detect and mitigate because they are powered by machines rather than humans. This makes it essential for businesses to adopt faster detection and response mechanisms.

How does Fortinet address these evolving cyber threats with your products and services?

Fortinet has been investing in its security fabric for over a decade to ensure seamless integration between Fortinet products and third-party vendors. This integration is crucial in providing a unified defence system. AI-powered security solutions help accelerate detection times and improve response capabilities, providing a more robust defence against machine-powered threats.

How does Fortinet align with the theme of securing an AI-powered future, and how is the company using AI for proactive and reactive security measures?

AI has become ubiquitous, from mobile phones to security systems, and at Fortinet, the integration of AI into security solutions has been a priority for over a decade. The aim is to accelerate threat detection and response times, ultimately reducing the mean time to detect and respond to threats. As cybercriminals also use AI to execute attacks, it is crucial for Fortinet to stay ahead with AI-enabled security solutions.



How are cybercriminals utilising AI to exploit vulnerabilities, and how is Fortinet counteracting these efforts?

Cybercriminals are also leveraging AI for their attacks. For example, they use AI to create personalised phishing campaigns that are harder to detect. AI is also used to automate the creation of zero-day exploits, enabling fast and widespread attacks. Fortinet uses AI to enhance detection, response, and mitigation

capabilities, particularly against attacks generated by AI.

What cybersecurity recommendations would you give to organisations in the Middle East as they look towards 2025?

Integration is key. The security architecture should focus on seamless integration of technologies to reduce detection times. AI must be embedded in security design from the beginning

to minimise the time between detecting a breach and responding to it. Organisations in the Middle East are encouraged to invest in integrated solutions that leverage AI to secure their environments and ensure their security products work together cohesively.

What are Fortinet's next steps in advancing AI-enabled security?

Fortinet will continue to invest in AI and machine learning to enhance its security fabric. The goal is to embed AI capabilities into all products, from intrusion prevention systems to endpoint protection. The ultimate aim is to provide real-time, actionable insights that allow businesses to detect and mitigate threats faster, even as these threats grow in sophistication. 📌

AI-POWERED SECURITY SOLUTIONS ARE CRUCIAL TO ACCELERATE THREAT DETECTION AND RESPONSE, ALLOWING BUSINESSES TO STAY AHEAD OF INCREASINGLY SOPHISTICATED, MACHINE-DRIVEN CYBERATTACKS.

STRENGTHENING CYBER RESILIENCE IN THE MIDDLE EAST

SULTAN MAHMOOD, CHIEF SECURITY AND PRIVACY OFFICER AT HUAWEI GULF NORTH, DISCUSSES AI-DRIVEN SECURITY SOLUTIONS AND THE IMPORTANCE OF COLLABORATION TO ADDRESS RISING CYBER THREATS WITH SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP.

The cybersecurity landscape in the Middle East is becoming increasingly complex, with businesses facing growing challenges from sophisticated cyber threats. Sultan Mahmood, Huawei's Chief Security and Privacy Officer for Gulf North, highlights the company's efforts to integrate AI into its security solutions and emphasises the need for collaboration between governments, enterprises, and technology providers to build stronger cyber resilience across the region.

GISEC Global is buzzing with energy, how does this year's vibe compare to previous years?

The increased turnout speaks volumes about the growing awareness and interest in cybersecurity. It's no longer just technologists attending, but also a wider cross-section of professionals from various industries. This shows that people are eager to understand how they can leverage these technologies for both business and personal success.

Cybersecurity threats are ever-evolving. What are the most significant threats to businesses in the Middle East right now?

The GCC and Middle East have seen a steady increase in threats, especially over the past year. Denial-of-Service (DoS) attacks have been prominent, targeting both enterprises and individuals. Ransomware attacks are also on the rise, and with the proliferation of AI, these threats are becoming even more sophisticated. The threat actors are more advanced, and attacks are becoming more multidimensional and complex. Businesses must take a holistic approach to safeguard against these emerging threats.

Huawei showcased some innovative solutions. Can you tell us more about them?

Huawei presented two flagship solutions this year. First, we demonstrated our AI capabilities at the Huawei Cloud section, where we show how AI can be harnessed to secure cloud environments. Second,

we're showcasing our Unified Secure Access Service Edge (SASE) solution, which combines cloud, network, edge, and endpoint protection, offering end-to-end security for enterprises. These solutions aim to provide comprehensive protection against the growing cybersecurity threats in the region.

How is Huawei collaborating with governments and enterprises to enhance cybersecurity resilience in the region?

Huawei's cybersecurity strategy has evolved over the past 30 years. We've



Sultan Mahmood
Chief Security and Privacy
Officer at Huawei Gulf North.

always prioritised delivering secure, trustworthy products to our customers. However, we recently realised that individual efforts are not enough. That's why we introduced our cybersecurity "three-door" strategy, focusing on the entire value chain. It emphasises collaboration between Huawei, our

customers, technology providers, and regulators. We believe cybersecurity is a collective effort, and resilience can only be achieved when all players in the ecosystem work together. Specifically, we're supporting national governments in enhancing their cybersecurity policies, offering our insights and solutions to

make their cyber resilience frameworks more effective.

What message would you like to share with the global InfoSec community attending GISEC about the future of cybersecurity in 2025 and beyond?

My message is simple: Collaborate, collaborate, collaborate. The cybersecurity landscape is too complex for any single entity to handle alone. We must work together to build a secure and resilient digital future for all. Only through collaboration can we ensure the success and protection of the digital ecosystem. 🇮🇪

CYBERSECURITY IS A TEAM SPORT. ONLY THROUGH COLLABORATION CAN WE ACHIEVE A SECURE AND RESILIENT DIGITAL FUTURE.
SULTAN MAHMOOD, HUAWEI GULF NORTH



Benny Czarny
Chief Executive Officer, OPSWAT.

**AI IS EMBEDDED ACROSS OUR ENTIRE
PLATFORM TO PROTECT CRITICAL
INFRASTRUCTURE FROM TODAY'S
MOST ADVANCED THREATS.**

OPSWAT SHARPENS CRITICAL INFRASTRUCTURE DEFENCE AT GISEC GLOBAL 2025

BENNY CZARNY, CHIEF EXECUTIVE OFFICER, OUTLINES OPSWAT'S INNOVATION PRIORITIES, AI-POWERED STRATEGIES, AND FOCUS ON CYBERSECURITY EDUCATION AT THE MIDDLE EAST'S FLAGSHIP SECURITY EVENT.

OPSWAT, a global leader in Critical Infrastructure Protection (CIP) cybersecurity solutions, marked a strong presence at GISEC Global 2025, further cementing its strategic commitment to the region.

Benny Czarny, Chief Executive Officer at OPSWAT, shared insights on how the company is advancing innovation, leveraging AI, building regional partnerships, and addressing the vital need for cybersecurity training and certification in critical infrastructure. In this exclusive conversation with Sandhya D'Mello, Technology Editor, CPI Media Group, Czarny highlights OPSWAT's priorities and how the company is helping enterprises stay ahead of an increasingly sophisticated threat landscape.

How do you view the evolution of GISEC Global 2025?

GISEC is fast becoming one of the notable global cybersecurity events, alongside the likes of RSA and Black Hat. What's exciting is the event's global expansion, with new editions coming up in Vietnam, Nigeria, Morocco, and more. We are very enthusiastic about our partnership with GISEC and its growing international reach.

What are your top strategic priorities to drive OPSWAT's business forward in the region?

Our key focus areas are twofold: product innovation and go-to-market execution.

We are committed to manufacturing an exceptional cybersecurity platform that protects critical infrastructure. This includes innovative technologies, a suite of integrated products, and a strong training academy. The second priority is how we bring these solutions to market through partnerships, branding, events like GISEC, sales activities, and build a strong presence in the region.

What technologies and solutions OPSWAT showcased at GISEC this year?

We demonstrated our entire platform at GISEC — over 23 products designed to protect critical infrastructure. To make complex security concepts more accessible, we have created simulated environments showcasing real-world scenarios, such as attacks on energy infrastructure. Visitors could see how attackers could target critical systems and, importantly, how our platform can detect, prevent, and mitigate such threats. It's a highly visual and impactful demonstration of the capabilities we bring to the table.

How does OPSWAT view innovation in the era of AI, and how is the company leveraging AI internally and in its products?

AI is embedded throughout our platform. We use AI engines to detect threats, classify file types, and power our data sanitisation technology. For example, if an attacker tries to use an AI-generated payload hidden in a JPEG

or a manipulated Word document, our technology regenerates clean versions of these files, neutralising potential risks.

In our adaptive sandbox and DLP solutions, AI identifies sensitive content in videos and images and applies redaction where needed to comply with privacy and security mandates. Internally, we use AI to accelerate everything from customer support chatbots to legal reviews, security questionnaires, marketing, and product development. AI enables us to enhance productivity and deliver better outcomes for our customers.

Why is training and certification a key focus for OPSWAT, and what initiatives have you launched in this space?

There are hundreds of cybersecurity certifications out there—423 to be precise, based on our analysis. Yet only one, our programme, is dedicated specifically to critical infrastructure. Most certifications are either product-specific or very generic.

Our academy was created to address this gap. It provides holistic training for IT and security professionals working in critical infrastructure—covering everything from PLC risks to secure data transfer practices. The response has been overwhelming, with hundreds of thousands of certified students and very positive feedback from both individuals and organisations. We are proud to contribute to both the protection of critical infrastructure and the career development of cybersecurity professionals in the region. 📌



**WE BELIEVE THAT NO SINGLE
COMPANY CAN HAVE ALL
THE ATTACK SIGNATURES
OR COVER ALL ATTACK
SURFACES, SO INTEGRATION
AND COLLABORATION ARE
CRUCIAL**

Saif AlRefai
Solutions Engineering Manager at
OPSWAT.

OPSWAT SHOWCASES CUTTING-EDGE CYBERSECURITY SOLUTIONS FOR CRITICAL SECTORS AT GISEC 2025

SAIF ALREFAI, SOLUTIONS ENGINEERING MANAGER AT OPSWAT, DELVES INTO THE FUTURE OF CYBERSECURITY FOR CRITICAL INFRASTRUCTURE, HIGHLIGHTING AI-DRIVEN PROTECTION AND THE UAE'S PROACTIVE STANCE ON SECURING VITAL SECTORS IN AN INTERVIEW WITH SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP.

At GISEC 2025, Saif AlRefai of OPSWAT shared valuable insights into the evolving world of cybersecurity, particularly in the protection of critical infrastructure. With the increasing reliance on technology and AI, securing sectors such as energy, oil, gas, and government has never been more important. AlRefai discusses the role of AI, multi-layered security measures, and the UAE's commitment to staying ahead of cyber threats. In this interview, he outlines how OPSWAT is leading the charge in the fight against cyber risks.

Can you walk us through some of the key technologies OPSWAT is showcased at GISEC this year?

We showcased a range of technologies this year, including our OPOD experience labs and critical infrastructure protection labs. We're also highlighting our OT and cross-domain cybersecurity solutions, which are central to what we're doing at OPSWAT. It's really exciting to present these solutions, which are designed to tackle the most pressing security challenges in today's landscape.

What are the most common use cases for OPSWAT technology in the critical infrastructure sector?

In the Middle East, sectors like energy, oil and gas, government, and defence are top priorities for us, along with banking. Two use cases that stand out are peripheral media security and web application security. For example, our Metal Defender Kiosk handles peripheral media security, while our Metal Defender ICAP Server integrates seamlessly to provide web application file upload security. These solutions help ensure that organisations in critical sectors can operate securely.

How prepared are critical infrastructure entities in the UAE to defend against these cyber threats?

The UAE is one of the top countries globally when it comes to cybersecurity. The level of expertise, market maturity, and government support is impressive. There's real commitment from both the government and enterprise sectors to invest in cybersecurity. However, as we all know, cybersecurity is an ongoing battle. The landscape is constantly evolving, and threats are becoming more advanced, particularly with the rise of AI. However, overall, the UAE is in a very strong position and is one of the leading cybersecurity regions.

What is OPSWAT's approach to integrating AI in OT and IT security?

AI is no longer an option; it's a necessity.

At OPSWAT, we are focusing on two key strategies: first, using AI to protect against AI-driven attacks, and second, fostering collaboration and telemetry. We believe that no single company can have all the attack signatures or cover all attack surfaces, so integration and collaboration are crucial. Our multi-scanning solution, for example, integrates products from over 30 vendors, providing a comprehensive approach to security.

How is OPSWAT helping critical infrastructure entities in the UAE strengthen their cybersecurity defences?

Our approach is based on zero trust architecture, which prioritises prevention over detection. We treat any file or input source as potentially malicious from the outset, using multi-scanning and deep sanitisation to neutralise threats before they can cause harm. Additionally, we're using AI and machine learning to build baselines for network activity and detect abnormal behaviour. This is especially important in OT environments, where internet connectivity is limited, making signature-based updates difficult. AI plays a vital role in understanding what constitutes normal activity, enabling us to protect networks based on that knowledge. 🔒

COLLABORATION OVER COMPETITION POWERS FUTURE OF CYBERSECURITY, SAYS EVAD

ABDULLAH A. QAISI, CEO & GENERAL MANAGER OF EVAD, SHARES HOW COLLABORATION AND STORYTELLING ARE RESHAPING CYBERSECURITY DISTRIBUTION IN THE REGION.

The 14th edition of GISEC Global witnessed a remarkable convergence of cybersecurity leaders, with vibrant energy lasting through all three days of the event. Among the notable voices was Abdullah A. Qaisi, CEO & General Manager of EVAD, who reflected on the evolving cybersecurity landscape, both regionally and globally. Having just returned from RSA Conference in San Francisco, Qaisi brought a unique perspective to the table—highlighting how the Middle East, and particularly GISEC, is matching global standards in terms of scale, relevance, and impact in an exclusive interview with Sandhya D'Mello, Technology Editor, CPI Media Group.

Qaisi emphasised that cybersecurity today is less about product pitches and more about impactful storytelling and ecosystem collaboration. He underscored the importance of moving away from a siloed, competitive mindset toward a community-driven approach where distributors, vendors, and partners collectively raise awareness and readiness in the cybersecurity space.

How do you compare the energy and scale of GISEC 2025 with other global cybersecurity events?

Recently I attended RSA Conference in San Francisco, and coming from RSA to GISEC was a different kind of challenge—but a very exciting one. RSA is known for showcasing cutting-edge technologies, but I must say, coming back to Dubai and experiencing GISEC at this scale fills me with pride. This event truly matches international standards. Compared to last

year, GISEC 2025 has seen higher visitor turnout and more focused interactions. The arrangements have been seamless, making it easy to connect and engage. Even on the third day, the energy feels like day one.

What did EVAD showcase at GISEC Global 2025?

This is our first year exhibiting at GISEC, although we've been part of other events like GITEX in the past. Choosing GISEC this year was the right move—its cybersecurity focus aligns perfectly with our position as a value-added distributor in the field. The audience here knows what they want, and that made it easier to present our offerings. At I[VAD], we believe cybersecurity isn't just a product to sell—it's a story to tell. We've focused on storytelling to help customers understand their needs and how our solutions fit.

The cybersecurity distribution space is growing fast. How do you view this evolution and competition?

Competition is intense, but I don't see other distributors as competitors. I see them as partners in building a stronger cybersecurity community. If one distributor grows, it benefits the entire ecosystem. For example, where EVAD is strong—like the UAE, Saudi Arabia, or even Kenya—we help others gain ground, and vice versa. This shared growth enriches the community. It's about collaboration, not combat. Our collective goal should be to raise awareness and understanding of cybersecurity together.

That's an inspiring perspective. How

do you foster this mindset across the cybersecurity community?


We need to stop operating in silos. I had a recent experience at our booth where a client arrived with a distributor. The moment I introduced myself, the distributor said they couldn't engage as they were from a competing firm. I told them, "Let's collaborate. If I can't close the deal, maybe you will. Or maybe we do it together." That mindset shift—from competition to cooperation—is key. If your competitor is doing well, don't pull them down—rise to their level. Together, we can build a safer ecosystem.

What challenges still exist in making cybersecurity more relatable?

The issue is that people outside the cybersecurity world still see us as a cost rather than a safeguard. That's because the domain is complex and often poorly understood. To change this perception, we need more storytellers. We must humanise cybersecurity through storytelling—explain it in ways that resonate with real business needs. Once we do that, understanding and investment will follow naturally.

What technologies do you think will define the future of cybersecurity distribution?

Looking ahead, I see the biggest growth in areas like IoT security, threat intelligence, AI-powered solutions, and penetration testing. But above all, data security is emerging as the most critical domain. It has been neglected for too long. Today, it must be recognised as a standalone security pillar, just as vital as network or endpoint security. Data security will be central to future strategies. 🔑



**WE MUST HUMANISE
CYBERSECURITY THROUGH
STORYTELLING—EXPLAIN
IT IN WAYS THAT RESONATE
WITH REAL BUSINESS
NEEDS. ONCE WE DO THAT,
UNDERSTANDING AND
INVESTMENT WILL FOLLOW
NATURALLY.**

Abdullah A. Qaisi, CEO & General Manager of EVAD.

KASPERSKY'S CYBER IMMUNITY VISION PROTECTS CRITICAL INFRASTRUCTURE, SHAPES THE FUTURE OF SECURITY

TOUFIC DERBASS, MANAGING DIRECTOR FOR THE MIDDLE EAST, TÜRKIYE, AND AFRICA AT KASPERSKY, SHEDS LIGHT ON THE CHALLENGES OF SECURING CRITICAL SECTORS AND THE COMPANY'S PIONEERING CYBER IMMUNITY APPROACH.

Cybersecurity threats are evolving at a rapid pace, and industries such as utilities, oil and gas, and manufacturing are increasingly exposed due to outdated systems. Kaspersky, a global cybersecurity and digital privacy company, is responding to these vulnerabilities with innovative solutions, spearheading a movement toward cyber immunity.

Toufic Derbass, Managing Director for the Middle East, Türkiye, and Africa, spoke to Sandhya D'Mello, Technology Editor, CPI Media Group at Gisec Global 2025 on how the company is tackling the unique challenges facing critical infrastructure sectors, the transformative role of AI in cybersecurity, and the shift from traditional security measures to proactive, unhackable systems. Derbass also explores Kaspersky's leadership in defining the future of cybersecurity through its vision of cyber immunity.

Why industrial sectors like utilities, oil and gas, and manufacturing are more vulnerable to cyberattacks, and how Kaspersky is addressing these challenges?

Critical infrastructure, such as utilities, oil and gas, and manufacturing, often

lags behind traditional IT environments in terms of cybersecurity maturity. Industries are more vulnerable because they typically rely on older, less secure systems that weren't designed with modern cybersecurity threats in mind. For example, in the Middle East, we see that about 38% of devices in the industrial sector have been compromised. At Kaspersky, we focus on providing a full portfolio that covers both endpoint and network protection for these sectors. Additionally, we offer dedicated threat intelligence and operate the world's only CERT for industrial cybersecurity, which allows us to provide specialised support to address these unique challenges.


Can you explain Kaspersky's concept of 'cyber immunity.' How does it contrast with conventional cybersecurity approaches?

Cyber immunity goes beyond traditional cybersecurity. While cybersecurity is about detecting and mitigating risks, cyber immunity aims to make systems completely unhackable. This vision is about building secure technology by design, ensuring that devices are inherently secure and resistant to cyberattacks. Kaspersky's goal is to move beyond the ongoing cycle of attacks and defenses. For instance,

we've developed cyber-immune thin clients and applications that are secure by design, even in the face of AI-driven threats. This methodology ensures that systems remain resilient, even in highly vulnerable environments like banking or telecommunications. It's a transformative approach, and while we're still in the early stages, we are leading the way in executing this vision.

Could you share your thoughts on how AI is changing the landscape of cyber threats, and how Kaspersky is utilising AI to stay ahead of these threats?

AI is a double-edged sword in the world of cybersecurity. On the one hand, cybercriminals are leveraging AI to automate and scale their attacks, creating highly credible phishing campaigns and malicious files. In fact, at Kaspersky, we identify around 500,000 malicious files per day, a number that would be impossible to handle manually. On the other hand, we've been using AI and machine learning for over 20 years, long before AI became a buzzword. Our solutions utilise AI to predict and stop threats in real time, analysing vast amounts of data to detect anomalies and respond quickly. AI allows us to manage the sheer volume of attacks and ensure that our systems are continuously evolving to meet new challenges.



Toufic Derbass, Managing Director for the Middle East, Türkiye, and Africa at Kaspersky.

WE OFFER DEDICATED THREAT INTELLIGENCE AND OPERATE THE WORLD'S ONLY CERT FOR INDUSTRIAL CYBERSECURITY, WHICH ALLOWS US TO PROVIDE SPECIALISED SUPPORT TO ADDRESS THESE UNIQUE CHALLENGES.

You've mentioned that some cyberattacks on critical infrastructure have escalated to the level of cyber warfare, with real-world consequences. How can organisations prevent such catastrophic events from occurring?

Cyberattacks on critical infrastructure can indeed have devastating real-world consequences, such as explosions or system failures that disrupt entire industries or nations. Prevention starts with a proactive approach. Organisations must prioritise cybersecurity in their industrial environments, especially since many of these sectors are still catching up in terms of security measures. At Kaspersky, we emphasise the need for robust defense systems that not only detect but also prevent attacks before they can cause harm. We also stress the importance of collaboration between vendors, regulators, and other stakeholders to create a unified front against such advanced threats. By addressing cybersecurity at the design level, we can create more resilient systems that are capable of withstanding even the most sophisticated attacks.

Kaspersky has pioneered the development of cyber immunity. Could you discuss how this vision is being executed and how it's impacting the cybersecurity industry?

Cyber immunity is a long-term vision, and we are already taking steps to execute it. We've introduced cyber-immune products such as thin clients and an ecosystem of secure applications that provide a higher level of protection than traditional cybersecurity measures. This shift is gradually transforming the cybersecurity landscape, as we move from a reactive to a proactive stance, where systems are inherently immune to cyber threats. While we are still in the early stages of this transformation, especially in regions like Asia Pacific and the Middle East, we are leading the charge in creating these solutions. It's a game-changer, and it's changing how we think about security, moving us toward a future where attacks are no longer inevitable but preventable. 🔒

SENTINELONE'S AI-DRIVEN SOLUTIONS TRANSFORM CYBERSECURITY OPERATIONS AT GISEC GLOBAL 2025

MERIAM ELOUAZZANI SPOKE TO SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP ON HOW SINGULARITY HYPERAUTOMATION, AI SIEM, AND PURPLE AI ARE REVOLUTIONISING SECOPS, ENHANCING THREAT DETECTION, AND ADDRESSING MIDDLE EAST COMPLIANCE CHALLENGES.

Meriam ELOuazzani, Senior Regional Director for META at SentinelOne, shares insights into how the company's AI-driven innovations, including Singularity Hyperautomation, AI SIEM, and Purple AI, revolutionise cybersecurity operations, helping organisations improve threat detection, response times, and overall security efficiency. ELOuazzani discussed the growing demand for automation in cybersecurity, the importance of data accuracy, and the role of AI in transforming non-specialists into proficient security analysts. At GISEC Global 2025, SentinelOne showcased its "Mortal vs. Machine" experience, demonstrating the power of AI in enhancing security operations.

Can you walk us through the launch of Singularity™ Hyperautomation, AI SIEM, and Purple AI, and how these innovations are transforming cybersecurity operations?

Over the past year, we've seen a significant shift in the approach from CIOs and CISOs who now come to us with a more defined understanding of their needs. Previously, they would approach us with interest in our XDR (Extended Detection and Response) solutions, but often without a specific focus on key areas like cloud features, identity management, or the application of AI and automation. This year, however, they are coming with a targeted mindset, seeking information on specific advancements in hyperautomation and related capabilities. Interest in Purple AI has also grown, with the technology now becoming a tangible

reality. This shift has led to an increasing enthusiasm for integrating these innovations into cybersecurity strategies, enabling organisations to refine and enhance their security operations.

How is AI revolutionising SecOps, and what impact is it having on organisations' ability to detect and respond to threats more quickly and efficiently?

AI is fundamentally transforming SecOps by enhancing organisations' ability to detect and respond to threats more swiftly and efficiently. From the outset, our company has integrated AI into detection, protection, and response, recognising that traditional signature-based approaches are no longer sufficient, especially given the prevalence of zero-day attacks. SentinelOne has consistently prioritised AI-driven solutions for detection and response, and we continue to enhance these capabilities with additional modules that increase the relevance and effectiveness of AI. A key advancement is the integration of AI into the way cybersecurity analysts interact with data. By enabling analysts to query data using simple language—similar to

SENTINELONE HAS CONSISTENTLY PRIORITISED AI-DRIVEN SOLUTIONS FOR DETECTION AND RESPONSE, AND WE CONTINUE TO ENHANCE THESE CAPABILITIES WITH ADDITIONAL MODULES THAT INCREASE THE RELEVANCE AND EFFECTIVENESS OF AI.

how one would interact with ChatGPT—we make the process of correlating and analysing data more intuitive. These queries are then translated into advanced queries in the backend, streamlining the investigative process. Moreover, the system allows analysts to save and share these queries in notebooks, fostering collaboration among team members. This collaborative feature not only promotes consistency across the team but also accelerates the adoption of our technology. Ultimately, the use of AI reduces detection and response times, while simplifying automation, making security operations more efficient and effective in today's fast-paced threat landscape.

What are the key cybersecurity threats and compliance challenges organisations in the Middle East are facing, and how is the shift towards automation helping to address these issues?

Organisations in the Middle East are facing several key cybersecurity threats and compliance challenges, particularly around data accuracy, correlation, and the integration of data into a single platform. While automation plays a crucial role in addressing these challenges, it is essential that the data feeding into AI models is properly formatted, accurate, and up-to-date. Without proper data training and ingestion, the potential for incorrect interpretations increases, leading to lower-quality results.

Automation remains a central focus in organisations' cybersecurity strategies, making it crucial to not only emphasise its role but also address the need for robust data correlation and accuracy. By ensuring that data from multiple sources is properly integrated and queried through a unified platform, organisations can enhance the quality of their security operations and improve their ability to detect and respond to threats more effectively. Automation, combined with accurate data, is essential for organisations to meet



Meriam ElOuazzani, Senior Regional Director for META at SentinelOne.

the growing demands of cybersecurity while navigating the complexities of compliance.

With the growing need for autonomous security, how does SentinelOne's AI-driven threat detection and unified protection help organisations secure their infrastructure, and can you explain the "Mortal vs. Machine" experience at GISEC Global 2025?

SentinelOne's AI-driven threat detection and unified protection offer organisations an autonomous approach to securing their infrastructure. The system analyses data to detect anomalies or malicious activity, automatically identifying threats without human intervention. This allows for rapid

detection and response, significantly reducing the time and resources required for manual monitoring. At GISEC Global 2025, the "Mortal vs. Machine" experience aims to demonstrate the power of AI in transforming individuals into advanced security specialists. By leveraging AI tools, even someone with no prior cybersecurity knowledge can query data in plain English. The system then translates these queries into advanced queries in the backend, providing detailed threat-hunting results. This hands-on experience shows how AI can empower non-specialists, turning them into proficient analysts capable of identifying and responding to cyber threats effectively. 🔒

NOZOMI NETWORKS ENHANCES CRITICAL INFRASTRUCTURE SECURITY AMID EVOLVING CYBER THREATS

ANTON SHIPULIN, INDUSTRIAL CYBERSECURITY EVANGELIST AT NOZOMI NETWORKS, DISCUSSES THE COMPANY'S APPROACH TO SAFEGUARDING CRITICAL INFRASTRUCTURE AND ADDRESSING THE RISE OF AI-DRIVEN CYBER RISKS.

The cybersecurity landscape is rapidly changing, with digital technologies increasingly integrated into industrial control systems. This digital transformation has introduced new risks, especially with the rise of AI-driven cyber threats. Nozomi Networks is leading the way in securing critical infrastructure, offering solutions that ensure comprehensive protection across OT, IoT, IT, and wireless assets. In this interview, Anton Shipulin, Industrial Cybersecurity Evangelist at Nozomi Networks, discusses with Sandhya D'Mello, Technology Editor, CPI Media Group, how the company addresses evolving threats and helps organisations comply with stringent regulatory requirements while safeguarding critical and renewable infrastructure.

How does Nozomi secure critical infrastructure in the region amid evolving cybersecurity threats, and how does it contribute to improving operational efficiency?

Critical infrastructure is vital for a nation's cybersecurity and the functioning of the country. Essential services such as water, electricity, and oil and gas energy rely heavily on these systems, and it is crucial to ensure their continuous,

uninterrupted operation. With the rapid digital transformation and the integration of advanced technologies into control systems managing critical infrastructure, these systems are increasingly dependent on digital components. However, this dependence introduces new risks.

Unauthorised access and potential cyberattacks pose significant threats to these systems, as malicious actors can exploit vulnerabilities to gain control. It is crucial to monitor these systems closely and identify any deviations from normal operations. Detecting cyberattacks, process anomalies, or other irregular behaviours at an early stage is essential for maintaining security and ensuring the longevity of these facilities.

Nozomi Networks addresses these challenges by providing real-time monitoring of network traffic, process telemetry, vulnerabilities, and asset changes within industrial control systems. This approach allows for the timely detection of anomalies and attacks, enabling prompt responses to

safeguard critical infrastructure and ensure its resilience.

How can organisations achieve full-spectrum protection across OT, IoT, IT, and wireless assets, and what solutions does Nozomi offer to address these complex security challenges?

Our primary focus is on securing industrial control systems and cyber-physical systems, including the Internet of Things (IoT). When it comes to industrial control systems, they often comprise a variety of components, including pure OT elements like controllers and PLCs, as well as IT components such as network devices, routers, switches, PCs, laptops, and servers running traditional operating systems like Windows.

It is critical not to focus solely on protecting OT systems. Rather, organisations must ensure protection across all components surrounding these critical systems. To address this, our solution expands beyond just supporting OT protocols. While we

NOZOMI OFFERS COMPREHENSIVE SOLUTIONS THAT FOCUS ON ASSET DISCOVERY, THREAT DETECTION, AND VULNERABILITY IDENTIFICATION.



Anton Shipulin, Industrial Cybersecurity Evangelist at Nozomi Networks.

excel in supporting OT protocols with deep packet inspection for anomaly detection and attack identification, we also support IT systems and the most common IT protocols like DNS, SNMP, and others. This is achieved through passive network monitoring, which ensures visibility across both OT and IT environments.

For enhanced asset visibility and discovery, we've added active discovery components, including smart polling, which queries devices for details. Additionally, we've expanded our solutions to incorporate various types of sensors, including network sensors and recently, endpoint sensors. These endpoint sensors can be deployed on systems such as Windows, Linux, and MacOS, especially in areas where

network sensors cannot be installed.

Furthermore, with the increasing adoption of wireless networks in industrial environments, it is essential to monitor and protect these networks to prevent unauthorised access. In some cases, clients may prohibit wireless networks entirely. However, even in such scenarios, monitoring wireless communications remains vital to detect unauthorised devices, such as rogue wireless access points or USB dongles, that could pose a security risk.

Overall, Nozomi offers a comprehensive solution that ensures protection across wireless networks, wired networks, and endpoints, providing organisations with full-spectrum security across their OT, IoT, IT, and wireless assets.

With the rise of AI-driven cyber threats, how do you see the threat landscape evolving, and what steps is Nozomi taking to stay ahead of these emerging risks?

The rise of AI technologies is both a beneficial and accelerating force for cybersecurity, but unfortunately, it is also being exploited by cybercriminals to enhance their attacks. Attackers leverage AI for tasks such as vulnerability scanning, spam generation, and even coding attacks. This makes it easier for them to create new and more sophisticated attacks, accelerating the pace of the threat landscape.

For organisations, this presents a significant challenge, as AI-driven threats allow attackers to quickly evolve their methods, making it critical for asset

owners to detect these attacks in a timely and precise manner. This is where Nozomi Networks focuses its efforts. Our solution is not only designed for network detection but also for understanding industrial and IoT protocols, which is crucial in accurately identifying attacks.

As the frequency and complexity of attacks grow, the amount of data that needs to be processed increases exponentially, making it harder to correlate and analyse all the relevant information. To address this challenge, we integrate AI and machine learning into our platform for alert correlation and generating insights. These technologies help us manage and analyse vast amounts of data, allowing us to detect threats more effectively.

Moreover, as more industrial automation vendors and cloud providers implement AI-based systems, it is essential to protect these components from potential threats. AI-based systems themselves are now vulnerable, and our focus includes monitoring attempts to attack these systems, ensuring that they are adequately safeguarded.

Nozomi is adapting to the evolving threat landscape by incorporating AI and machine learning for better threat detection and data processing, while also expanding our focus to protect AI-based systems in industrial automation and cloud environments.

Could you share insights into Nozomi's complete cyber-physical protection offerings, particularly in securing

critical and renewable infrastructure? How do your solutions enable compliance in highly regulated sectors?

Nozomi's solution focuses on comprehensive monitoring across a wide range of environments, including wireless networks, endpoint activities, and IoT systems. Our offerings include a diverse set of sensors for network, wireless, and endpoint monitoring, alongside management components for on-premises environments and cloud-based components for information collection and analysis.

By providing real-time visibility and continuous monitoring, our solutions ensure that critical infrastructure, including renewable energy systems, is secured against potential cyber threats. Furthermore, our solutions help organisations meet the compliance requirements of highly regulated sectors by ensuring that all systems are continuously monitored, vulnerabilities are detected early, and appropriate actions are taken to mitigate risks in real time.

How does Nozomi ensure compliance with highly regulated sectors, especially considering the growing number of cybersecurity frameworks and regulations globally?

Compliance with cybersecurity regulations is increasingly important, with various frameworks emerging across the globe, such as those in Europe, the United States (e.g., New York City's cybersecurity regulations), and other regions. One of the key elements of compliance is ensuring proper asset discovery, asset management, threat detection, and vulnerability management.

To help organisations meet these regulatory requirements, Nozomi offers comprehensive solutions that focus on asset discovery, threat detection, and vulnerability identification. By addressing these key components, our solutions ensure the security of critical networks and data, enabling organisations to comply with regulations while also enhancing their overall cybersecurity posture. 🔒





Fortify Your Cybersecurity

Fortinet
Global Cybersecurity Leader

The Fortinet Security Fabric is the industry's highest-performing cybersecurity platform, delivering broad, integrated, and automated cybersecurity capabilities supported by a large, open ecosystem. The Fortinet Security Fabric empowers organizations to achieve secured digital acceleration outcomes by reducing complexity, streamlining operations, and increasing threat detection and response capabilities.

Learn more at fortinet.com



Bernard Montel, EMEA Technical Director and Security Strategist at Tenable.

TENABLE CHAMPIONS PROACTIVE CYBERSECURITY WITH BUSINESS-ALIGNED EXPOSURE MANAGEMENT

BERNARD MONTEL, EMEA TECHNICAL DIRECTOR AND SECURITY STRATEGIST AT TENABLE, OUTLINES HOW EXPOSURE MANAGEMENT, AI, AND UNIFIED DATA ARE TRANSFORMING CYBER DEFENSE STRATEGIES IN THE MIDDLE EAST.

Tenable —the Exposure Management company— emphasised a paradigm shift in cybersecurity, from reactive detection to proactive exposure management. Bernard Montel, EMEA Technical

Director and Security Strategist, explains how Tenable's strategic acquisitions, innovative AI-driven tools, and unified platform approach are helping businesses understand and reduce cyber risk from a business perspective.

In this interview with Sandhya D'Mello, Technology Editor, CPI Media Group, Montel dives deep into Tenable's latest capabilities, including vulnerability intelligence, attack path analysis, and the growing role of AI in anticipating and mitigating threats

What did Tenable showcase at GISEC Global 2025?

We focused on three core elements. First is exposure management, which is our strategic direction, especially after a key acquisition in February. It's about understanding exposures from a business risk lens, transitioning from traditional vulnerability management to holistic attack surface visibility. Second, we demonstrated how exposure management can proactively identify open paths that attackers might exploit. Third, we aimed to change the mindset in cybersecurity from reactive to proactive, helping organisations reduce complexity and improve risk-based decision-making.

Can Tenable predict and block attacks in real time using AI?

We differentiate between reactive and proactive cybersecurity. While most organisations invest heavily in detection and response (reactive), Tenable is rooted in proactive defense. We don't detect active attacks—we detect paths that could lead to an attack. By identifying and closing these paths, we help prevent potential breaches before they occur. This shift helps reduce the need for overly complex detection systems and allows security teams to focus on meaningful risk mitigation.

Could you share an anonymised use case where exposure management prevented significant damage?

Absolutely. We've helped clients reduce ransomware risk by detecting exposure paths aligned to specific emerging threats. One recent case involved a top-down response—where

a CISO, alarmed by news of an ongoing ransomware campaign, asked whether their organisation was exposed. Our platform quickly identified attack paths and exposures related to that campaign, enabling rapid remediation and preventing potential impact.

How does exposure management enhance operational efficiency for security teams?

It's a game-changer. By investing in proactive measures, organisations reduce the number of detection rules and simplify incident response workflows. For example, once we detect an open attack path, we can initiate tailored actions—investigate if it's already been exploited or activate specific response protocols. This seamless integration with Security Operations Centers (SOCs) significantly boosts operational efficiency.

What new features are being introduced in Tenable's Security Center, and how do they improve security posture?

We've enhanced our platform with vulnerability intelligence. This gives users access to 20 years of Tenable research and threat data—before scanning even begins. Instead of scanning first and analysing later, we provide context-rich insights upfront. This enables faster decision-making and more effective prioritisation. We've also opened the platform to third-party sources to enrich context, making our exposure management platform even more powerful.

With increasing demand for OT security, how is Tenable addressing

regional cybersecurity challenges?

We were pioneers in recognising IT/OT convergence, starting back in 2019. Today, we go beyond IT and OT to include IoT and cloud in a unified risk view. Given the region's critical infrastructure sectors—utilities, oil and gas, and transport—we offer visibility from factory floor to cloud. Our unique ability to link all these environments within the Tenable One platform gives unmatched insight into how attackers could exploit interconnected systems.

How is Tenable integrating AI into its defense strategy, particularly with the rise of GenAI?

AI isn't new for us—we've used machine learning for years in scoring vulnerabilities and misconfigurations. With GenAI, we're enhancing that further. For example, attackers are already using GenAI to generate malware. On the defense side, we use GenAI to simplify complex attack paths, contextualise risk, and generate tailored remediation advice. Our chatbot interface, trained on our vulnerability intelligence database, helps security practitioners understand their exposures faster and more clearly.

Which technologies are shaping the future of exposure management?

Exposure management is becoming the next-generation cybersecurity framework. Gartner's CTM (Continuous Threat Exposure Management) is a strong validation of this. Key technologies include multi-source data integration (from both Tenable and third parties), advanced analytics, and automated workflows with playbooks for contextual response. Most importantly, the evolution is moving toward business-aligned risk visibility—empowering C-level decision-makers with clear answers to the question: "Is my business exposed today?" 📌

BY INVESTING IN PROACTIVE MEASURES, ORGANISATIONS REDUCE THE NUMBER OF DETECTION RULES AND SIMPLIFY INCIDENT RESPONSE WORKFLOWS

ManageEngine UNVEILS AI-POWERED UNIFIED CYBERSECURITY SOLUTIONS AT GISEC GLOBAL 2025

DRIVING UNIFIED, AI-POWERED CYBERSECURITY TO COMBAT
EVOLVING THREATS AND SECURE THE AI-DRIVEN FUTURE.

The evolving cybersecurity landscape in the Middle East highlights trends such as state-sponsored cyberattacks, ransomware-as-a-service, and supply chain vulnerabilities.

In an interview with Sandhya D'Mello, Technology Editor, CPI Media Group, Sujoy Banerjee, Associate Director at ManageEngine, discussed key challenges, including the shortage of skilled professionals and fragmented security tools, emphasising ManageEngine's commitment to unified, AI-powered platforms that enhance threat detection, response, and compliance at GISEC Global 2025.

ManageEngine showcased its integrated solutions, including SIEM, PAM, and endpoint protection, designed to simplify security operations and empower organisations to secure their AI-driven future.

What are the key cybersecurity trends you're observing in the region, and how do these trends impact organisations as they strengthen their security posture?

While this is a part of a global trend, in this region, we're particularly observing a sharp rise in state-sponsored cyberattacks, as well as ransomware-as-a-service (RaaS). The sophisticated threats are evolving rapidly, making



Sujoy Banerjee, Associate Director at ManageEngine.

them harder to detect and defend against.

At the same time, there's a growing awareness around supply chain vulnerabilities, which are now seen as critical risk vectors that organisations can no longer afford to overlook. Additionally, the broader adoption of cloud infrastructure, especially local cloud solutions, is a positive development, but at the same time it introduces new complexities from a security perspective.

All these factors combined are driving demand for more unified and proactive security solutions. Organisations are now looking beyond traditional defenses and seeking integrated platforms that can help them detect, respond to, and mitigate threats across their entire ecosystem in real time. The evolving trends are pushing businesses to rethink their strategies and adopt a more holistic approach to security.

What are some of the biggest challenges organisations in the Middle East are facing when it comes to cybersecurity, and how is ManageEngine helping them address these issues?

There are multiple challenges in today's cybersecurity landscape. One major issue is the shortage of skilled cybersecurity professionals, which continues to impact organisations across the region. Another key challenge lies in managing and maintaining hybrid infrastructure environments, which add layers of complexity to security operations.

However, the most critical gap right now is the fragmented nature of existing security solutions. Many

organisations still operate in silos, with disconnected tools and systems that don't communicate effectively. This fragmentation makes it extremely difficult to gain a unified view of threats and respond efficiently.

This is exactly where ManageEngine is focusing its efforts by building a unified security platform. We're working across our entire product portfolio to address these gaps. Whether it's Privileged Access Management (PAM), Security Information And Event Management (SIEM), or unified endpoint security, our goal is to bring everything together onto one comprehensive secure platform. This will help organisations simplify their security operations, improve visibility, and strengthen their overall cybersecurity posture.

Could you elaborate on ManageEngine's theme at GISEC Global 2025 and what specific innovations or solutions you showcased during the event?

Today, AI is no longer just a buzzword or a "good to have," it's become an essential part of any organisation's cybersecurity strategy. We've been integrating AI into our solutions for quite some time, not just in the cybersecurity domain but across our entire product portfolio.

From a GISEC 2025 perspective, our focus is on encouraging organisations to adopt a unified security portfolio. We want to help them consolidate their tools and gain clearer visibility into their threat landscape. Our aim is to show how AI-powered insights from our solutions can enhance threat detection, provide a deeper understanding of potential vulnerabilities, and offer a more proactive approach to cybersecurity.

We're also emphasising how our integrated solutions, including SIEM, PAM, and endpoint protection, work together to create a cohesive security framework. Ultimately, we are looking to empower organisations to detect, analyse, and respond to threats faster and more effectively through a unified, AI-driven platform.

How do your AI-powered phishing simulation, AI-driven threat prediction, and automated response mechanisms work together to create a robust security framework for organisations, and how is ManageEngine helping businesses secure their AI-powered future?

We focus on three key aspects: simulation, prediction, and automation.

Simulation involves gathering data from various sources to proactively analyse potential threats. By simulating different attack scenarios, we can assess and predict what types of threats might emerge. This proactive approach enables us to stay ahead of potential risks.

Next, prediction comes into play. We use the collected data and advanced AI-driven insights to predict upcoming threats. This system-driven approach helps us identify potential vulnerabilities and threats more accurately and in real-time, providing organisations with a clearer understanding of what they might face.

Finally, the third element is automation, with the insights gathered through simulation and prediction, we leverage automation to enhance the response mechanism. This allows us to streamline threat detection and response, making the entire process faster and more efficient.

Our product portfolio is designed to help organisations not only address their cybersecurity needs but also ensure compliance with local regulations, offering tailored solutions that meet regional requirements and provide organisations with a more secure and compliant framework. 📌

ORGANISATIONS ARE NOW LOOKING BEYOND TRADITIONAL DEFENSES AND SEEKING INTEGRATED PLATFORMS THAT CAN HELP THEM DETECT, RESPOND TO, AND MITIGATE THREATS ACROSS THEIR ENTIRE ECOSYSTEM IN REAL TIME.

CROWDSTRIKE UNVEILS AI INNOVATIONS SHAPING CYBER DEFENSE AT GISEC 2025

YASSIN WATLAL, HEAD OF SYSTEM ENGINEERING AND SOLUTIONS ARCHITECT META AT CROWDSTRIKE, SHARES KEY TAKEAWAYS FROM GISEC 2025, SHEDDING LIGHT ON AI-DRIVEN CYBER THREATS AND DEFENSE INNOVATIONS.



Yassin Watlal, Head of System Engineering and Solutions Architect META at CrowdStrike.

During GISEC Global 2025, discussions centered on Artificial Intelligence (AI) and its transformative impact on cyber threats, with Yassin Watlal, Head of System Engineering and Solutions Architect META at CrowdStrike, offering insights to Sandhya D'Mello, Technology Editor, CPI Media Group, on growing sophistication of cyber attackers using AI.

Watlal, explored the evolving strategies to counter these advanced threats, from AI-enhanced phishing attacks to insider threats like Famous Chollima. Additionally, Businesses could secure their systems and adapt to rapid technological innovations, addressing the evolving cybercrime landscape, AI's role in defense, and practical security measures to mitigate risks.

How has GISEC been this year compared to last year, would you like to share some insights?

GISEC Global 2025 fostered significant engagement and insightful discussions this year, particularly focusing on the profound ways in which Artificial Intelligence (AI) is reshaping the landscape of cyber threats. Attendees actively participated in exploring the evolving tactics of threat actors leveraging AI, as well as the defensive strategies and innovative solutions being

developed to counter these sophisticated attacks. The conversations delved into the implications of AI for various aspects of cybersecurity, including threat detection, incident response, vulnerability management, and security automation. The level of engagement underscored the collective interest and concern within the cybersecurity community regarding the transformative impact of AI.

What are the key findings from the 2025 GTR that you would like to share with us?

Current threat actors possess significant funding and meticulously planned objectives in their campaigns. A notable emphasis on identity threats has been observed, evidenced by a 50% increase in dark web advertisements offering compromised credentials. This has led to expedited attacks, with an average breakout time of 48 minutes, defined as the time for initial machine infection and lateral movement. The fastest recorded breakout time was 51 seconds.

What is the role of Gen AI in modern cybercrime?

AI is utilised by cyber attackers to enhance their attacks, integrating it as a novel component within their global arsenal. Generative AI is primarily employed to refine emails prior to launching phishing campaigns, thereby improving their authenticity and appeal to recipients. Consequently, a significant increase in click-through rates has been observed, with AI-generated emails achieving a 54% click-through rate compared to a 14% rate for human-authored emails. This technology also reduces the skill threshold required for less sophisticated threat actors to engage in malicious activities.

Can you tell us more about the insider threats like Famous Chollima? What are some of the mitigation strategies companies can adopt?

The threat actor group Famous Chollima, based in North Korea, employs artificial intelligence to generate fraudulent applications, LinkedIn profiles, and candidate personas, meticulously crafting them to appear highly credible and attractive to recruiters and human resource personnel, aiming to secure employment. Furthermore, during the interview process, they utilise generative AI to formulate responses to questions, enabling them to successfully pass interviews. Instances have been reported wherein individuals associated with this group were hired, received company-issued laptops through intermediaries, and performed assigned tasks, effectively gaining insider access.

Can you tell us more about the companies that can secure cloud and hybrid environments?

AI-native platform, such as the CrowdStrike Falcon platform, is crucial for effective cybersecurity. Integrating AI natively allows for the realisation of its full benefits, particularly in enabling responses at machine speed. Given that attacks materialise rapidly, it is imperative to respond with equal speed. This ensures the ability to maintain a comprehensive understanding of the situation and effectively address threats in a timely manner.

What did CrowdStrike exhibit at GISEC this year?

We showcased our latest innovations, our Falcon platform, and discussing Charlotte AI, our generative AI offering and highlighted products that enhance the ecosystem.

What are the new technologies that will be integrated by CrowdStrike in the field of cybersecurity?

Artificial intelligence is progressively being integrated into various solutions, exemplified by the detection triage facilitated by Charlotte AI and the comprehensive agentic API, which significantly enhances efficiency for cybersecurity analysts. This implementation results in substantial time savings, approximately 40 hours per week for the team, by enabling the agentic AI to effectively differentiate between true positives and false positives, thus expediting response times and optimising the deployment of AI in the defense strategy.

How is cybersecurity being integrated with this rapid technological innovation, and what security measures should businesses adopt in response?

Our focus is on ensuring resilience and maintaining a proactive stance against threats. We aim to alleviate routine operational burdens, thereby mitigating risks for our clients. All our efforts are directed towards preventing breaches and safeguarding customer interests by streamlining operational processes traditionally associated with legacy systems. We believe Agentic AI should be deployed to handle these tasks.

Could you provide tips for best security practices?

We have observed attacks such as LLM jacking. When deploying AI, it is imperative to secure it throughout the deployment process, rather than deploying without security considerations. It is necessary to ensure the security of these new application layers. Regarding LLM jacking, if threat actors obtain cloud credentials, they can log in and execute queries within a subscribed LLM. This can result in increased costs and potential data exposure. Data could be compromised, and private knowledge could be extracted through techniques such as prompt injection. Securing AI and this new application layer is of significant importance. Crowdstrike can provide assistance in this regard. 📌

GENERATIVE AI IS PRIMARILY EMPLOYED TO REFINE EMAILS PRIOR TO LAUNCHING PHISHING CAMPAIGNS, THEREBY IMPROVING THEIR AUTHENTICITY AND APPEAL TO RECIPIENTS.

QUANTUMGATE SHAPES CYBERSECURITY IN UAE; PREPARES FOR QUANTUM FUTURE

JANNE HIRVIMIES, CHIEF TECHNOLOGY OFFICER AT QUANTUMGATE, DISCUSSES THE GROWING ROLE OF CYBERSECURITY IN THE REGION AND EMERGING CHALLENGES IN THE AGE OF QUANTUM COMPUTING.

The cybersecurity landscape in the Middle East, particularly in the UAE, has seen a remarkable transformation in recent years. QuantumGate's Chief Technology Officer, Janne Hirvimies, spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, on how cybersecurity is evolving, the impact of quantum computing, and the solutions his company is offering to stay ahead of emerging threats.

How do you see the evolution of cybersecurity trends in the past few years, especially in the UAE and the Middle East?

I have been in the ecosystem since 2016, and I've witnessed significant growth, especially in the past few years. The UAE, in particular, has been at the forefront of driving this transformation. The country has not only been investing

heavily in its tech ecosystem but also introducing groundbreaking regulations. One example is the Blockchain and Quantum Computing (BQC) regulation, which has positioned the UAE as a leader in cybersecurity strategy on the global stage.

How are QuantumGate's products and solutions aligned with the UAE's cybersecurity strategy?

QuantumGate is a part of the ATRC ecosystem, which ensures that our products and solutions are fully aligned with the UAE's cybersecurity strategy. We have been proactive in anticipating regulatory needs, even three years ahead of time. Leaders like Dr. Najwa Aaraj have driven initiatives that have shaped the development of data security products, ensuring they are in line with both upcoming regulations and the needs of the industry.



What emerging cybersecurity threats or trends do you foresee impacting enterprises in the Middle East in the coming years?

Over the past 25-30 years, the security landscape has been largely shaped by traditional cryptographic methods. However, with the rise of quantum computing, the paradigm is shifting. The approach to cryptography will need to be reinvented, as it has been largely stable and secure for decades. Many enterprises still don't have clear ownership over cryptographic assets. A



Janne Hirvimies, Chief Technology Officer at QuantumGate.

collective responsibility model won't work anymore, and organisations will need to start managing cryptographic assets properly, identify their gaps, and build a roadmap for the future.

Can you highlight any innovative technologies that QuantumGate showcased at GISEC?

At GISEC, we showcased two main product families. One is a full solution

for managing cryptographic assets tailored to the needs of the UAE and the region. This is a novel solution because traditionally, cryptography has been scattered across various parts of an enterprise without centralised management. We are offering a structured approach to understanding and managing this. The second solution addresses the emerging requirements of post-quantum data security and communication security, ensuring that organisations are ready for the next generation of cybersecurity challenges. 

ORGANISATIONS WILL NEED TO START MANAGING CRYPTOGRAPHIC ASSETS PROPERLY, IDENTIFY THEIR GAPS, AND BUILD A ROADMAP FOR THE FUTURE.

REDEFINING CYBERSECURITY DISTRIBUTION WITH AI-DRIVEN INNOVATION ENHANCES THREAT DETECTION, AUTOMATES SECURITY RESPONSE

BURHAN ABU BAJA AND **ABDURRAHMAN NAJAR** OF NXTHOP TECHNOLOGIES SHARE INSIGHTS ON EVOLVING DISTRIBUTION PATTERNS, CYBERSECURITY GOVERNANCE FRAMEWORKS, AI-DRIVEN INNOVATION, CLOUD ADOPTION, AND ACCELERATING TECH TRANSITIONS IN THE REGION.

NXTHOP Technologies is strategically positioning itself as a key player in the evolving cybersecurity landscape by leveraging AI-driven innovation, customized deployment models, and alignment with regional governance frameworks, as highlighted during GISEC Global 2025. With insights from leaders like Burhan Abu Baja, Chief Solution Sales Strategist, and Abdurrahman Najjar, VP of Sales of NXTHOP Technologies, shared insights with Tahawultech.com on how NXTHOP is addressing these paradigm shifts. NxtHop plays a key role in guiding enterprises through paradigm shifts in cybersecurity by facilitating the adoption of cybersecurity solutions and enabling seamless transitions from traditional infrastructures, which enhances digital resilience across the region. These shifts, driven by advancements like AI, have transformed threat detection, prevention, and response strategies, requiring organizations to adopt more adaptive, intelligent security frameworks.

How has cybersecurity distribution evolved in recent years, and what role is NXTHOP Technologies playing in this transformation?

Burhan Abu Baja: In recent years, cybersecurity distribution has rapidly evolved, with the region experiencing a condensed timeline of maturity driven by urgent needs across devices, apps, and cloud access, highlighting the challenge of system compatibility and reliance on APIs. Burhan Abu Baja emphasizes that NXTHOP Technologies plays a pivotal role in this transformation by bridging these gaps through innovative, AI-powered solutions capable of defending against increasingly sophisticated cyber threats, embodying the principle that only AI can combat AI.

With so many cybersecurity solutions in the market, how can a business identify the right one, especially across different sectors like startups, SMEs, and conglomerates?

Abdurrahman Najjar: There's no one-size-fits-all in cybersecurity. governments within the region have invested significantly

in building strong cybersecurity governance frameworks tailored to industries—whether financial, governmental, or critical infrastructure. Our advice: follow these national frameworks. They offer a solid starting point and ensure alignment with compliance and best practices.

What sets NXTHOP's distribution model apart from others in the region?

Burhan Abu Baja: We focus on filling market gaps by offering a comprehensive portfolio of complementary products rather than competing ones. Our solutions are AI-driven and tailored to business needs. We work closely with partners and customers to align technologies with business objectives, ensuring value, innovation, and healthy margins, without engaging in price wars. We are strictly channel-driven, never selling direct, which ensures focus and support at every stage.

How do you support businesses in transitioning from traditional to modern cybersecurity solutions?

Abdurrahman Najjar: We provide



**Abdurrahman Najjar, VP of Sales, NXTHOP Technologies and
Burhan Abu Baja, Chief Solution Sales Strategist, NXTHOP Technologies.**

**OUR SOLUTIONS
ARE DESIGNED TO
INTEGRATE EASILY,
AND OUR CHANNEL
PARTNERS ENSURE
→ SWIFT EXECUTION,
REDUCING
TRANSITION TIME
SIGNIFICANTLY.**

deployment models suited for every need—cloud, on-premise, or hybrid. Cloud deployment is immediate and adaptable to customer scenarios. On-premise takes slightly longer due to the necessary infrastructure requirements. Hybrid models are ideal for sectors with regulatory constraints.

Have you observed a shift in customer preference toward cloud-based cybersecurity solutions in the region?

Burhan Abu Baja: Yes, cloud adoption is clearly growing. There are regulatory mandates in countries like Saudi Arabia and the UAE that are accelerating this shift. Even conservative sectors like banking are embracing cloud because of updated compliance standards. NXTHOP ensures all our solutions—whether cloud or on-prem—adhere to national and international cybersecurity regulations.

What's your final message to enterprises navigating today's cybersecurity complexity?

Abdurrahman Najjar: Be proactive. Cyber threats are evolving rapidly, and cyber hackers are leveraging technology faster than most organizations. By aligning with national regulatory frameworks and working with trusted technology business partner like NXTHOP and their vendors and channels; businesses can stay protected and resilient. 🔑



THE CALIBER OF PROFESSIONALS NEEDED FOR CRITICAL INFRASTRUCTURE IS DIFFERENT FROM THE TYPICAL IT SECURITY WORKFORCE, AND THIS MAKES SECURING THESE SYSTEMS EVEN MORE COMPLEX.

Ilya Leonov, Regional Director of Positive Technologies.

INNOVATIONS IN OT SECURITY: POSITIVE TECHNOLOGIES PAVES THE WAY FOR A SAFER TOMORROW

ILYA LEONOV HIGHLIGHTS INNOVATIVE DEMONSTRATIONS, CHALLENGES IN SECURING CRITICAL INFRASTRUCTURE, AND THE UAE'S ROLE IN BUILDING A SECURE FUTURE FOR GLOBAL TALENT AND BUSINESSES.

Ilya Leonov, Regional Director of Positive Technologies, provided valuable insights into the company's groundbreaking contributions to the cybersecurity landscape at GISEC Global 2025 to Sandhya D'Mello, Technology Editor, CPI Media Group.

From showcasing sophisticated attack vectors to focusing on the complexities of securing operational technology (OT) and critical infrastructure, Ilya shared the unique challenges faced by the industry. In this interview, he also discussed the shortage of skilled resources in cybersecurity and the UAE's emerging role as a global hub for talent and secure business environments. Below, we explore his thoughts on the evolving cybersecurity landscape.

Can you tell us about some of the innovative things Positive Technologies showcased at GISEC Global 2025 this year?

We showcased some very unique technical demonstrations. One of the highlights was a direct memory access attack, where we showed how you can unlock a laptop without knowing the password. It looks like magic, but it's actually quite simple and sophisticated at the same time. Another interesting demonstration is a fault injection attack, where we manipulate the voltage of a motherboard to trick encryption systems and unlock devices. We've received a lot of interest in these sophisticated attack vectors, as not many companies can perform these types of demonstrations.

How is your company focusing on OT security this year?

This year, we focused heavily on OT (Operational Technology) security, which has become increasingly important, especially with the growing emphasis on critical infrastructure. At GISEC Global, we had a dedicated area for critical infrastructure, and contributing to that was showcasing application security, network security, and monitoring tools that helped identify abnormal activities in the systems. The tools were specifically designed for the unique and complex environments that critical infrastructure operates in.

What challenges do you see in securing critical infrastructure and OT systems?

Securing critical infrastructure is quite challenging due to a combination of factors. One of the biggest challenges is the legacy systems still in use, such as outdated versions of Windows like XP, which are still running in some industrial environments. This makes it difficult to implement modern security measures. Additionally, the personnel working in OT environments often lack the specialised knowledge required for effective cybersecurity. The caliber of professionals needed for critical infrastructure is different from the typical IT security workforce, and this makes securing these systems even more complex.

Is there a gap in the skills and resources available for securing critical infrastructure, and how can this gap be addressed?

The shortage of skilled resources is a major pain point in the industry. The gap between the basic knowledge required and the specialised skills needed to protect critical infrastructure is significant. While there are initiatives from governments and private companies to address this gap, there's still a lot of work to be done. The rapid pace of technological advancements, especially in cybersecurity, makes it difficult to keep up. Bridging this gap requires ongoing efforts in upskilling and reskilling talent.

Do you believe the UAE has the capacity to attract global talent and create a safer environment for businesses?

I believe the UAE is doing an excellent job at creating the right conditions and environment to attract international talent across various fields, not just cybersecurity. If the right conditions are in place, it becomes a winning strategy to build a safer future. Since I've been here, I've seen how the government and the country have been focusing on creating these opportunities for professionals. In the long run, I believe this will yield tremendous results for the country.

Can we say that the UAE is a gateway to building a secure future?

The UAE is positioning itself as a gateway to building a secure tomorrow, both in terms of attracting talent and providing a conducive environment for businesses. It's creating a significant difference in securing the future for both talent and enterprises. This is something that will have a lasting impact, and I strongly believe the UAE will continue to lead in this area. 🇦🇪



WE MUST MOVE AWAY FROM CHASING BREACHES AND INSTEAD FOCUS ON PERSISTENTLY PROTECTING DATA ITSELF—THIS SHIFT TO DATA-CENTRIC SECURITY CHANGES THE GAME FOR THE REGION.

Justin Endres
Chief Revenue Officer at Seclore.

SECLORE REDEFINES DATA-CENTRIC SECURITY TO TACKLE NEXT-GENERATION CYBER THREATS

I SECLORE UNVEILED AI-POWERED INNOVATIONS AND A STRATEGIC VISION FOR SECURING DIGITAL ASSETS AS MIDDLE EAST ENTERPRISES ACCELERATE THEIR CYBER RESILIENCE JOURNEY.

The Middle East's digital economy is booming, but so too are the complexities of cybersecurity in an AI-driven world. At GISEC Global 2025, Seclore showcased how data-centric security is fast becoming an essential foundation for safeguarding critical information. Speaking at the event, the company's Chief Revenue Officer shared perspectives on key trends, emerging threats with Sandhya D'Mello, Technology Editor, CPI Media Group, on how Seclore is collaborating with government and enterprise stakeholders to elevate cyber resilience across the region.

How did Seclore's presence at GISEC align with your broader cybersecurity strategy for the region?

Our mission has always been to help large enterprises protect their most critical digital assets. GISEC gave us the perfect opportunity to demonstrate this commitment, while also listening to the unique needs of customers and partners in the region. With bold digital transformation agendas shaping markets like Saudi Arabia and the UAE, cybersecurity is a growing priority—and we are here to support that journey with proven innovations.

What emerging cybersecurity threats or trends do you believe will most significantly impact enterprises in the Middle East in the coming year?

Insider threats continue to pose significant risks, and the complexity of third-party ecosystems only compounds the challenge. Data leakage is now a universal concern. With AI adoption accelerating, often without the necessary governance or visibility, enterprises face even greater risks. To stay ahead, organisations must rethink their approach—focusing on protecting the data itself through data-centric security, rather than relying solely on traditional infrastructure defences.

Can you highlight any innovative technologies or solutions Seclore showcased at this year's event?

We were excited to showcase several key advancements. Our expanded data-centric security platform now includes automated policies to safeguard sensitive documents interacting with AI environments. We also enhanced our risk insights to give organisations better visibility into data flows and potential exposure. Additionally, we have deepened our integrations with top ecosystem partners, including Symantec, Skyhigh,

and Forcepoint—delivering even greater value through collaborative cybersecurity.

How is Seclore collaborating with government and enterprises to strengthen cyber resilience across sectors?

Our collaboration has been built over many years of close engagement with public and private sector stakeholders. Beyond delivering leading solutions, we are helping drive a strategic shift from infrastructure-centric to data-centric security models. This aligns well with national digital transformation goals, such as Saudi Arabia's Vision 2030, where cybersecurity is rightly being embedded into every layer of the digital economy.

What would be your message to the cybersecurity community today?

We must evolve our thinking. The days of perimeter-focused defences are behind us. The future lies in persistent protection of data—wherever it resides, moves, or is shared. The region's shift toward cloud, AI, and ecosystem-driven collaboration demands this proactive approach. Moving to data-centric security puts us ahead of the curve and enables us to protect what truly matters in an increasingly complex threat environment. **I**

SECLORE'S SAUDI ARABIA JOURNEY POWERS REGIONAL CYBERSECURITY GROWTH

URAZ FARUKH, VICE PRESIDENT – SAUDI & BAHRAIN AT SECLORE, SPOKE TO SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP ON HOW THE COMPANY BUILT A STRONGHOLD IN THE KINGDOM BY ALIGNING WITH NATIONAL REGULATIONS AND NURTURING LOCAL TALENT.

GISEC Global 2025 served as the ideal backdrop to hear how Seclore's presence in Saudi Arabia evolved from a single-client operation to a robust regional force. The company's journey reflects the Kingdom's transformation into a global cybersecurity leader, driven by strict compliance mandates and a strong focus on data protection. In this exchange, Uraz Farukh, Vice President – Saudi & Bahrain, discusses building local talent, the role of regulators like the NCA, and how both Saudi Arabia and the UAE are shaping the Middle East's cyber future.

Could you share insights on how you built Seclore's presence in Saudi Arabia?

I've been in the IT domain in Saudi Arabia for over 25 years. I came across Seclore around 11 years ago, at a time

when digital rights management was still a niche concept and the market wasn't ready. We started modestly and got our first customer in 2014. Over the years, the market matured rapidly. With strong support from Seclore's senior management and co-founders who believed in the region, we've built a solid foundation. Today, we have over 35 employees on the ground, our own regional headquarters—complying with Saudi Arabia's regulatory requirements—and a robust mix of Saudi and non-Saudi talent. We've especially invested in young Saudi graduates, training resident engineers, and integrating them into customer-facing roles to enhance the secure experience we offer.

How do you view Saudi Arabia's proactive role in strengthening the region's cybersecurity landscape?

The Saudi cybersecurity market is

extremely mature, covering all key areas—firewalls, data protection, and more. The National Cybersecurity Authority (NCA) has mandated all entities—government, semi-government, and corporate—to comply with cybersecurity regulations. Compliance is not optional, which is why Saudi Arabia is globally recognized as a leader in cybersecurity practices. We aligned closely with NCA requirements and collaborated with other regulators such as





Uraz Farukh, Vice President – Saudi & Bahrain at Seclore.

SAMA, CITC, CMA, and Aramco, which has its own vendor cybersecurity guidelines. All of these regulatory bodies place a strong emphasis on data protection, which aligns perfectly with our core focus.

How did GISEC 2025 compare to previous editions, especially in terms of energy and footfall?

I've been attending GITEX for the last 20 years, and GISEC since its inception. Every

year we thought it had reached its peak, but it just kept getting bigger. Last year at GITEX Morocco, I was amazed by the turnout.

GISEC Global 2025 offered a highly focused cybersecurity environment, providing an excellent platform for engaging with Saudi, UAE, and wider Middle East customers and partners. The event proved valuable for brand visibility and networking, supported by a fantastic marketing team that helped us maximise our presence.

Do you agree that Saudi Arabia and the UAE are shaping the cybersecurity landscape of the Middle East?

Saudi Arabia is significantly ahead in terms of cybersecurity maturity, thanks to the well-established regulatory framework. The UAE is quickly advancing with evolving cybersecurity guidelines. Together, both countries are the main forces steering the regional cybersecurity agenda. 📌

GREEN CIRCLE DRIVES AI-FIRST CYBERSECURITY INNOVATION AT GISEC GLOBAL 2025

MOHAMMAD ALKHUDARI, FOUNDER AND CEO OF GREEN CIRCLE, UNVEILED THE REGION'S FIRST AI CYBERSECURITY RESEARCH CENTRE AT GISEC GLOBAL 2025 AND SHARED PIONEERING STRATEGIES TO COMBAT RISING CYBER COMPLEXITY ACROSS THE MIDDLE EAST.

Cybersecurity complexity is growing exponentially, with organisations in the Middle East and beyond seeking solutions that can match the speed and sophistication of AI-driven threats. At GISEC Global 2025, Green Circle positioned itself at the forefront of this transformation. Founder and CEO Mohammad Alkhudari shared with Sandhya D'Mello, Technology Editor, CPI Media Group, the company's strategic focus on AI-powered cybersecurity, the launch of an AI Cybersecurity Research Centre, and a vision for proactive collaboration with governments and enterprises to secure critical sectors.

How did Green Circle's presence at GISEC Global 2025 align with your broader cybersecurity strategy for the region?

Our focus has been on addressing one of today's biggest challenges in

cybersecurity — complexity. With so many vendors and products in the market, many organisations are overwhelmed. We are helping them simplify, manage, and operate their security more effectively. A key part of this is how we respond to AI: both the threats it introduces and the opportunities it offers. At GISEC, we showcased our solutions and vision, including our AI Cybersecurity Research Centre, which will help address this complexity.

What emerging cybersecurity threats or trends do you believe will most significantly impact enterprises in the Middle East and beyond in the coming years?

There are two major areas of concern. Internally, the complexity of environments and the number of internal threats are increasing, particularly with the rise of AI-driven tools. Many organisations still focus primarily on

external threats, but internal risks are growing fast. Externally, AI-driven attacks are becoming more sophisticated, which is why we are developing tactical solutions to counter them effectively.

Could you highlight some of the innovative technologies or solutions that Green Circle showcased at GISEC this year?

We began by presenting our strategy and vision — which we believe must come before solutions. Organisations need to define how they will work with AI, how they will automate their response and prevention capabilities. From this foundation, we announced the region's first AI Cybersecurity Research Centre, which will be based in our office in Dubai and





Mohammad Alkhudari, Founder and CEO of Green Circle.

run in partnership with leading local and international organisations and vendors. In terms of solutions, we showcased our AI-driven SOC (SecOps) tools, pre-defence agents, AI-enhanced NDR, and AI-assisted ethical hacking tools. Our differentiation is not just in products, but in the research that supports them — looking at how AI will impact the market, government, and employment.

How is Green Circle collaborating with governments and enterprises to strengthen cyber resilience across key economic sectors?

Through our AI Cybersecurity Research Centre, we are working to automate and streamline services, helping reduce risk for government entities and enterprises facing advanced AI-driven attacks. We are also advising on how to enable

the next generation of cybersecurity professionals — those coming out of universities — to integrate AI skills into their work, ensuring they remain relevant in this fast-changing field.

What message would you like to share with the cybersecurity community attending GISEC about your vision for cybersecurity in 2025?

We are in the midst of a major transformation. Our message is simple: we must adopt AI for cybersecurity, and we must fight AI-driven threats with AI. Everyone should consider how AI can enhance their work, rather than seeing it only as a threat to their business or employment. It is about staying ahead of the curve and becoming part of the solution. 🔑

WE MUST ADOPT AI FOR CYBERSECURITY AND FACE AI-DRIVEN THREATS WITH AI. THE FUTURE BELONGS TO THOSE WHO EMBRACE THIS TRANSFORMATION. MOHAMMAD ALKHUDARI, FOUNDER AND CEO, GREEN CIRCLE

**THE ATTACKERS ARE
NOT GOING TO STOP. WE
MUST COLLABORATE,
SHARE INTELLIGENCE,
AND STAY PREPARED
AS A GLOBAL
CYBERSECURITY
COMMUNITY.**

Mandar Patil
Founding Member and SVP – Global
Sales and Customer Success, Cyble.

CYBLE'S AI-DRIVEN CYBERSECURITY VISION TAKES CENTER STAGE AT GISEC

MANDAR PATIL, FOUNDED MEMBER AND SVP – GLOBAL SALES AND CUSTOMER SUCCESS AT CYBLE, SPOKE TO SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP, ABOUT THE COMPANY'S CUTTING-EDGE AI-POWERED PLATFORM AT GISEC 2025, ADDRESSING RISING CYBER THREATS IN THE MIDDLE EAST. FROM PROACTIVE THREAT INTELLIGENCE TO UNIFIED VISIBILITY, CYBLE IS EMPOWERING ENTERPRISES, GOVERNMENTS, AND THE CYBERSECURITY COMMUNITY TO BUILD A SAFER DIGITAL WORLD.

How did you find the energy and atmosphere on the first day of GISEC compared to last year?

GISEC has been a very promising event. There was a lot of energy, with many attendees from across the Middle East. The vibe from the cybersecurity community was different this year. It was a great opportunity to reconnect and explore new ways to drive progress in the coming years.

How does Cyble's presence at GISEC Global 2025 align with your broader cybersecurity strategy for the region?

While Cyble has a strong presence globally, the Middle East holds particular importance for us due to its growth potential and market appreciation. Our vision for FY25 is to contribute toward making the digital world safer for everyone. We are moving beyond monitoring external threats to proactively enhancing security across the region.

What emerging cybersecurity threats or trends do you believe will significantly

impact enterprises in the Middle East?

We recently released a threat research report for the region and observed that BFSI and government sectors remain key targets. Attackers are exploiting the attack surface through impersonation, brand abuse, and social media manipulation. Activism is also at its peak, with many bad actors targeting UAE and other entities. To counter this, the cybersecurity community needs to collaborate and share intelligence to strengthen collective defence.

What innovative technologies is Cyble showcasing this year?

We showcased our fully AI-driven platform focused on providing unified visibility across the threat landscape. Our AI algorithms significantly reduce noise in threat intelligence. The Cyble platform integrates multiple technologies—threat intel platform, threat feeds, brand monitoring, attack surface management, and engineered response—into a single interface. This consolidation allows a single analyst to manage what would otherwise require five or six separate tools.

How is Cyble collaborating with governments and enterprises to strengthen cyber resilience across the region?

In addition to supporting enterprises and BFSI, we have created a dedicated government vertical to address national security needs. We work with national cybersecurity councils, law enforcement agencies, and other government bodies to provide intelligence from the dark web, open web, and social media. This intelligence helps in identifying threats such as activism, terrorism, and cybercrime. We also help law enforcement by creating digital personas to accelerate investigations.

What is your parting message to the cybersecurity community at GISEC this year?

GISEC has been an exciting event, and we will continue to be part of it. My message to the cybersecurity community is simple: threats will only continue to rise. Attackers won't stop. It is essential that we collaborate and share information to stay prepared and resilient. 🛡️

SECEON POWERS CYBER RESILIENCE WITH UNIFIED SECURITY AT GISEC 2025

CHANDRA SHEKHAR PANDEY, FOUNDER AND CEO OF SECEON INC., SHARES INSIGHTS ON PLATFORM TRACTION, DEMO SUCCESS, AND MIDDLE EAST EXPANSION WITH TAHAWULTECH.COM.

GISEC Global 2025 reflected a strong wave of momentum for cybersecurity innovators like Seceon Inc. With an integrated approach to threat detection and response, the company is drawing attention for its unified platform that simplifies and strengthens cyber resilience. Chandra Shekhar Pandey, Founder and CEO of Seceon, spoke with Sandhya D'Mello, Technology Editor, CPI Media Group, about the platform's real-time capabilities, the surge in booth engagement, and his vision for growth in the UAE and broader Middle East.

How would you describe GISEC this year compared to previous editions?

The mood is incredibly vibrant. Compared to last year, we're seeing a lot more footfall and excitement. We had around 400 booth visits on day one and our

team actively engaged with partners and industry leaders. What's encouraging is the recognition we're receiving—even though Seceon isn't a globally known brand yet, many attendees are aware of our platform and have come with positive feedback. That kind of recall doesn't happen by accident—it shows the groundwork is paying off.

What did you showcase at GISEC this year?

We are presenting our unified security platform, which integrates SIEM, SOAR, XDR, and security posture management into a single solution. The goal is to eliminate the need for 15 to 20 different security tools by offering real-time insights, threat detection, and automated response capabilities on one platform. It helps organisations stay audit-ready at all times and immediately flag anomalies for proactive action. So far, we've

conducted over 50 live demos today alone, across four demo stations. That level of engagement has been very exciting.

What is most critical to building cyber resilience while maintaining operational efficiency?

The key is comprehensive visibility. Organisations must be able to detect and respond to threats early—before they spread. If your security tools are siloed, your analysts are left trying to make sense of billions of data points, and that slows down response times. Our platform provides context and situational awareness, which enables faster, more accurate action. Without this, even the best products or teams can struggle, and both resilience and security are compromised.

Do you have any expansion plans in the UAE or wider Middle East region?

We operate 100% through our partners. We've already placed team members on the ground to ensure partners are empowered and customers receive full value. Our mission is to demonstrate real efficacy and ROI so customers can not only experience the benefits but also advocate for the solution based on their success. **1**

IF YOUR SECURITY TOOLS ARE SILOED, YOUR ANALYSTS ARE LEFT TRYING TO MAKE SENSE OF BILLIONS OF DATA POINTS, AND THAT SLOWS DOWN RESPONSE TIMES.



Chandra Shekhar Pandey, Founder and CEO of Seceon Inc.

SHAPING THE FUTURE OF EXPOSURE MANAGEMENT WITH AI, ANALYTICS, AND COLLABORATION

HEIMIR FANNAR GUNNLAUGSSON, CHIEF EXECUTIVE OFFICER AT NANITOR, SHARED INSIGHTS WITH TAHAWULTECH.COM ON EVOLVING CYBERSECURITY NEEDS, THE ROLE OF AI, AND STRATEGIC PARTNERSHIPS DURING HIS PARTICIPATION AT GISEC GLOBAL 2025.

Nanitor, a key player in internal IT security and exposure management, continued to make its presence felt at GISEC Global. Heimir Fannar Gunnlaugsson, CEO of Nanitor, spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, about the company's ongoing mission to simplify risk visibility, his views on the evolving cybersecurity landscape, and why partnerships and talent development are crucial to meeting tomorrow's challenges.

What did Nanitor showcase at GISEC Global 2025?

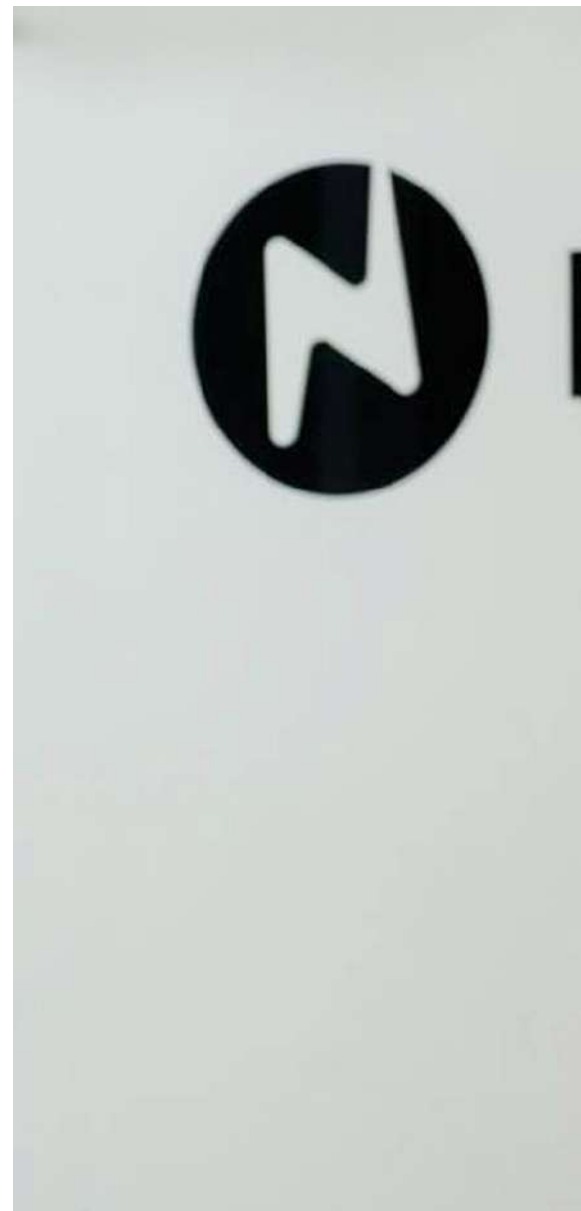
Nanitor is here primarily to support our

partners, engage with our distributors, and connect with customers. Our platform focuses on internal IT security, particularly in the area of exposure management. We detect and evaluate a wide range of internal security threats, giving our clients a simplified view of their risk posture. This differentiates us in the market and helps organisations act more decisively.

How was your experience been at GISEC this year compared to previous editions?

GISEC continues to be a dynamic and engaging platform. The footfall, energy, and discussions have been impressive. What stood out this year is the heightened

GISEC OFFERS A GOOD GLIMPSE INTO HOW THESE CROSS-SECTOR COLLABORATIONS ARE BEGINNING TO TAKE SHAPE



interest in AI—although many are still figuring out what it truly means for their businesses. There's a mix of curiosity and caution, and amid the excitement, the focus must remain on securing the fundamental IT infrastructure.

What role will emerging technologies play in shaping exposure management?

Technology is evolving rapidly in this field. Advanced scanning and deep analytics are now integral. At Nanitor, we are offering deeper insights than ever before. AI will certainly become a core part of this journey, bringing with it speed

Nanitor



Heimir Fannar Gunnlaugsson, Chief Executive Officer at Nanitor.

and predictive capabilities. I also foresee extensive collaboration across technology domains—asset discovery, threat detection, and external and internal risk management and these partnerships will drive more cohesive cybersecurity frameworks.

Can you elaborate on the importance of partnerships?

We expect partnerships to emerge across asset management, threat detection, exposure analysis, and internal-external security integrations. The alliances will be key to building a more comprehensive

exposure management ecosystem. GISEC offers a good glimpse into how these cross-sector collaborations are beginning to take shape.

What top trends do you foresee in exposure management for 2025?

First, AI will enhance speed and automation. Second, analytics will become more refined, offering actionable insights. Third, remediation strategies will evolve alongside these technologies. The process will grow more complex, but ultimately it will benefit customers by improving their ability to identify and

mitigate risks in real time.

Do you believe the industry has enough talent to support this rapid evolution?

Talent shortage remains a global challenge. The cybersecurity workforce is stretched thin, and most regions are competing for the same pool of professionals. While technology may fill some gaps, it is essential that we invest in education and hands-on training. Practical experience, not just theory, is critical. We must prioritise initiatives that build real-world skills to meet the demands of this evolving landscape. 🔑



CYNALYTICA PIONEERS CYBERSECURITY SOLUTIONS FOR CRITICAL INFRASTRUCTURE PROTECTION

THE COMPANY'S GROUNDBREAKING PLATFORM PROVIDES PASSIVE, REAL-TIME MONITORING FOR INDUSTRIAL CONTROL SYSTEMS, ADDRESSING DEEP-ROOTED CYBERSECURITY BLIND SPOTS IN CRITICAL INFRASTRUCTURE.

Cynalytica, a US-based cybersecurity company, is at the forefront of protecting critical infrastructure with its innovative approach to securing industrial control systems (ICS) and SCADA environments.

Led by CEO Richard Robinson, the company has introduced a groundbreaking platform that provides passive, real-time visibility across a wide range of control system communications, including analog, serial, and IP/Ethernet. The solution ensures comprehensive monitoring from Level 0 to Level 3 without disrupting operations. Robinson's vision has positioned Cynalytica as one of the few companies capable of addressing deep-rooted blind spots in critical infrastructure cybersecurity, setting a new standard for protection in the industry.

Robinson spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, during his visit to Dubai at GISEC Global 2025. He said: "Our primary focus has always been on education and raising awareness within the technology space, particularly as it relates to the protection of critical infrastructure. Several years ago, we founded our company with a specific purpose: to address a neglected segment of critical infrastructure that had been overlooked globally."

Robinson highlighted that the key issue is that, prior to the internet, essential infrastructure such as water, transportation, and power relied on

non-IP-based legacy communications. With the advent of the internet, the cybersecurity landscape has evolved, especially within industrial control systems. However, most cybersecurity companies focused solely on IP or Ethernet-based communications, overlooking the majority of critical infrastructure that remains non-IP-based. This gap still exists today.

"The impetus for founding this company was rooted in the Stuxnet incident, which is considered the first significant industrial control cybersecurity event. Stuxnet specifically targeted non-IP-based critical infrastructure components, highlighting a serious vulnerability in the industry. At the time, no technical solution existed to monitor these non-IP communications safely, and the challenge was clear: a new platform and technology had to be developed," he added.

"Unlike Ethernet-based systems, protecting non-IP communications required a different approach. While most companies avoided addressing this issue, our team—driven by expertise in this area—took on the challenge. Over the past seven to eight years, we have focused on developing solutions for this exact problem."

Cynalytica's primary customers to date have been the US government, mainly within the Department of Defense, who are acutely aware of the critical infrastructure systems that operate outside traditional IP networks and

require protection beyond internet-based cybersecurity tools.

"More recently, we have seen growing recognition within the industry that significant portions of critical infrastructure are not being adequately monitored, and that viable solutions are now available. Many professionals in the OT and industrial control spaces remain unaware that solutions to protect non-IP infrastructure exist. This is why we are actively engaging with industry stakeholders to raise awareness. It is gratifying to see that our efforts are gaining traction," said Robinson.

Cynalytica announced a strategic partnership with PwC Middle East, a development that marks significant recognition by a major global company in this field.

Jessica Ohnona, Executive Vice President of Data Science at Cynalytica, leads the development of machine learning and AI technologies that provide deep visibility into serial, analog, and hybrid OT environments—areas often overlooked by traditional security tools. Ohnona has been central to the company's growth strategy, product innovation, and market expansion across the US, the Middle East, and Europe.

Ohnona's work helps critical infrastructure operators strengthen cyber resilience without disrupting operations, while giving security stakeholders and investors' confidence in scalable, future-proof solutions.

Ohnona said: "At GISEC 2025, Cynalytica showcased how we're redefining visibility in OT cybersecurity—bringing real-time, passive monitoring to the deep layers of critical infrastructure that traditional tools overlook. As cyber-physical threats grow more sophisticated, especially across legacy and hybrid environments, this level of insight is no longer a luxury—it's essential. Together with PwC Middle East, we're accelerating resilience and delivering the operational assurance that infrastructure operators across the region—and the world—urgently need." 📌

UNLIKE ETHERNET-BASED SYSTEMS, PROTECTING NON-IP COMMUNICATIONS REQUIRED A DIFFERENT APPROACH. WHILE MOST COMPANIES AVOIDED ADDRESSING THIS ISSUE, OUR TEAM—DRIVEN BY EXPERTISE IN THIS AREA—TOOK ON THE CHALLENGE. OVER THE PAST SEVEN TO EIGHT YEARS, WE HAVE FOCUSED ON DEVELOPING SOLUTIONS FOR THIS EXACT PROBLEM.

VIRGINIA'S CYBER VISION FINDS MOMENTUM IN MIDDLE EAST

What happens when deep-rooted cybersecurity experience meets a region surging ahead in digital transformation? Anthony Perridge, Founder, First Mover Advantage, and Ellen Meinhart, Senior International Trade Manager, Northern Virginia Region, International Trade Virginia Economic Development Partnership, share with Sandhya D'Mello, Technology Editor, CPI Media Group, their perspectives on why the Middle East—particularly the UAE—is becoming a magnet for American cybersecurity innovation. From mentoring startups at GISEC to reflecting on the UAE's evolution into a global cyber hub, they shed light on talent gaps, strategic growth, and the power of long-standing relationships in a channel-driven market.

How did First Mover Advantage come into being, and what role will it play in the Middle East moving forward?

Anthony: About two years ago, I stepped back from work and took a year and a half off. During that time, I stayed busy—learning to read and play music, doing community gardening, and charity work. But eventually, I realized I wasn't ready to retire. I had decades of experience, a great network, and expertise, especially in helping North American cybersecurity startups grow internationally. So I decided to package that into a service: First Mover Advantage. My goal is to help cybersecurity companies expand globally, particularly in the Middle East—a region I know well. I don't want to work full-

time or for anyone; I want to work with exciting people and projects. We've brought six Virginia-based cybersecurity startups to GISEC this year, and I'm here to guide them, advising them on business practices, connecting them with the right partners, and helping them navigate the channel-centric and relationship-driven nature of this market.

How have you seen the UAE evolve over the years, especially in terms of cybersecurity and digital transformation?

Anthony: I was at the first ever GISEC in 2012 with Sourcefire. It was a small gathering back then. Today, it's bigger than some of the leading European cybersecurity expos. Dubai has grown into a major global hub—not just for trade, finance, and tourism—but now also for cybersecurity. It draws talent and companies from India, Africa, and Europe, aligning perfectly with the UAE's vision to be a global gateway and digital powerhouse.

What drove Virginia's decision to participate in GISEC, and how do you see the region as part of Virginia's long-term strategy?

Ellen: GISEC came highly recommended by other Virginia-based cybersecurity companies. This is our first time exhibiting here, although we've been to Infosecurity Europe in London several times. The Middle East, particularly the UAE, is very attractive due to its commitment to becoming a cybersecurity leader. The region is investing in talent

and technology and is positioning itself like the Silicon Valley of cybersecurity. That's appealing to Virginia companies.

Is there a cybersecurity skills gap in the Middle East, and how can it be addressed?

Ellen: There's a global cybersecurity skills gap, not just in the Middle East. Even in Virginia—which has the highest number of cybersecurity workers in the U.S.—many roles remain unfilled. We brought companies like Cyber Guru and ISC2 to GISEC because they focus on cybersecurity training and certifications. Building a skilled workforce is critical everywhere, and these companies help train individuals who want to enter the field. The Middle East's focus on developing local talent is impressive and timely.

What are your personal reflections as a woman in the cybersecurity space, and how can more women be encouraged to enter this field?

Ellen: I'd love to see more women in cybersecurity. My daughter is a programmer, but cybersecurity is different—it's more like strategic problem-solving or counterattack planning. It's exciting and dynamic, and it offers opportunities in sales, tech, and marketing. The key is awareness. Once women understand the scope and possibilities, more will be drawn to the field. I believe events like the women's breakfast at GISEC help raise that awareness, and I hope to see continued progress. **I**



Anthony Perridge, Founder, First Mover Advantage, and Ellen Meinhart - Senior International Trade Manager, Northern Virginia Region, International Trade Virginia Economic Development Partnership.

WE BROUGHT SIX COMPANIES TO GISEC, AND THEY'VE ALL HAD STRONG INTEREST AND ENGAGEMENT FROM POTENTIAL PARTNERS AND CLIENTS.



Yahya Kassab
Senior Director and General Manager – KSA, Gulf
Commvault.

CYBER RESILIENCE TOOK CENTRE STAGE AS GISEC EVOLVED INTO A GLOBAL CYBERSECURITY HUB

YAHYA KASSAB, SENIOR DIRECTOR AND GENERAL MANAGER – KSA, GULF, COMMVAULT, REFLECTED ON THE GROWING SIGNIFICANCE OF GISEC AND SHARED INSIGHTS WITH TAHAWULTECH.COM ON BUILDING SMARTER CYBER STRATEGIES.

GISEC 2025 concluded its 14th edition with resounding energy and engagement, drawing cybersecurity professionals, business leaders, and technology innovators from across the globe.

Yahya Kassab, a seasoned cybersecurity expert and regional head at Commvault, reflected on the evolution of the event, the shift in regional cybersecurity awareness, and the importance of resilience in today's AI-driven threat landscape.

Kassab shared Commvault's key highlights at the event, addressed emerging cyber challenges, and offered his top recommendations for companies aiming to strengthen their cyber posture in an exclusive interview with Sandhya D'Mello, Technology Editor, CPI Media Group.

How was GISEC Global 2025 compared to previous editions?

GISEC Global 2025 was arguably the only event in the region that brought together the entire cybersecurity ecosystem—vendors, partners, and customers. Collaboration remained essential to defending against cyberattacks, and the forum provided the ideal opportunity

to engage with stakeholders, discuss concerns, and explore mutual support. It truly served as a powerful gathering.

Do you remember your first GISEC? How had the event evolved since then?

I first attended GISEC in 2012, during its second year. From the outset, it offered something distinct to the cybersecurity community. Over time, the event grew—not just in scale but in relevance. Today, it attracts attention from both IT and security professionals, as well as business leaders across various sectors. Cybersecurity is no longer solely an IT issue; it impacts every aspect of business. That's why we now see a far more diverse, international audience attending.

What did Commvault showcase at GISEC this year?

This year, we participated alongside CPX, one of our largest partners, to emphasise the critical role of cyber resilience in complementing cybersecurity and cyber defence. We engaged in several discussions aimed at educating customers on why cyber resilience had become indispensable. We also prepared to launch a new service to help customers remain protected from cyberattacks. While I couldn't disclose

full details at the time, an announcement was on the horizon.

What were your top three recommendations for companies developing their strategy?

First, acknowledge the necessity of a cyber resilience plan. Many organisations had yet to reach this stage.

Second, build a robust ecosystem. No organisation can do everything alone. Whether it's vendors, systems integrators, or service providers, the right partners must align with your strategy.

Third, constantly revalidate your plan. Cyber resilience isn't static. With the threat landscape continually evolving, your approach must be dynamic and responsive. Ultimately, it's about who can outsmart whom.

You've often stressed the importance of awareness. Why is it so vital?

Awareness formed the foundation. It wasn't just the responsibility of the IT team, but of the entire organisation—across business units and among end users. Anyone could become a potential entry point for a cyber threat. Keeping everyone informed and alert was a fundamental aspect of safeguarding the enterprise. 🛡️

FINESSE BOLSTERS CYBERSECURITY WITH AI-POWERED SOC AND ADVANCED PENETRATION TESTING

PRADEEP KRISHNAN NAIR, VICE PRESIDENT – IT SECURITY, FINESSE AND WALID FAOUR, SENIOR SECURITY CONSULTANT, FINESSE, DISCUSS WITH SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP, HOW THEIR 24/7 AI-DRIVEN SOC AND COMPREHENSIVE VPT SERVICES, INCLUDING IOT, API, AND ATM PENETRATION TESTING, EMPOWER CLIENTS TO SECURE THEIR DIGITAL INVESTMENTS AND THRIVE IN THE AI ERA.

With cybersecurity risks intensifying in the AI era, forward-thinking enterprises are seeking proactive and intelligent solutions to protect their digital assets. Finesse, a leading digital transformation enabler in the region, is strengthening its security offerings with an AI-powered Security Operations Center (SOC) and a comprehensive suite of Vulnerability Assessment and Penetration Testing (VAPT) services.

In a joint conversation, Pradeep Krishnan Nair, Vice President – IT Security, and Walid Faour, Senior Security Consultant at Finesse, share how the company is leveraging AI and advanced testing methodologies to help clients build cyber resilience, secure critical infrastructure, and stay ahead of evolving threats.

How does your MSSP help businesses protect their digital assets and brand reputation in the AI era?

Pradeep Krishnan Nair: We are recognized as a trusted digital system integrator in the region. Our Managed



OUR AI-POWERED SOC TRANSFORMS CYBERSECURITY FROM A TECHNICAL FUNCTION INTO A STRATEGIC BUSINESS ENABLER—PROTECTING NOT JUST IT SYSTEMS, BUT BRAND TRUST AND DIGITAL INVESTMENTS.

Security Services Provider (MSSP) offering includes a 24/7 AI-driven SOC that not only monitors but also contextualises threats from a business perspective. We ensure the protection of critical digital assets—including storage, Identity and Access Management (IAM), and SaaS applications—through real-time threat intelligence and attack surface management. Our proactive model aligns cybersecurity with business goals, providing comprehensive protection across the digital landscape.

How can your MSSP reduce the business impact of cyberattacks with AI-driven capabilities?

Pradeep Krishnan Nair: Our SOC leverages AI to scale over 120 use cases with intelligent automation. This results in enhanced threat detection, smarter trending engines, improved endpoint detection and response (EDR), faster malware reverse engineering, and more effective analysis of phishing emails. By automating threat hunting and streamlining analysis, we offer a significant advantage to clients in minimising the operational and reputational impact of cyber incidents.

How do you help business leaders make smarter and faster decisions about cyber risk using AI?

Pradeep Krishnan Nair: We integrate advanced Large Language Models (LLMs) and AI connectors—both industry-leading and in-house developed—into our security framework. These tools help business leaders interpret cyber risks in real-time and make informed decisions. Our mission is



to guide clients securely through their AI transformation journey, enabling them to adopt emerging technologies with confidence.

Finesse Cyberhub offers VAPT services. Can you describe what services are included?

Walid Faour: We offer a wide range of penetration testing services tailored to meet diverse client needs. This includes IoT security testing, web and mobile application penetration testing, API security assessments, hardware testing, and even specialised services like ATM and Wi-Fi penetration testing for the banking sector. Whether it's software or hardware, we ensure thorough evaluation across all attack vectors.

How does Finesse differ from the competition in penetration testing and offensive security?

Walid Faour: Our competitive edge lies in our highly skilled team. Beyond certifications and years of experience, our consultants actively engage in CVE research, bug bounty programs, and Capture the Flag (CTF) challenges. Many are recognised in global Hall of Fame listings for identifying critical vulnerabilities. This deep technical expertise enables us to uncover high-impact vulnerabilities that others may overlook, delivering greater value to our clients.

How is Finesse keeping up with AI in the realm of offensive security?

Walid Faour: AI plays a central role in our offensive security strategy. We automate many internal processes, from vulnerability discovery to exploit research. This not only accelerates our delivery timelines but also enhances the depth and accuracy of our testing. By integrating AI into our methodologies, we maintain a leading edge in the cybersecurity space and continue to offer timely, effective, and intelligent solutions to our clients. 📌

WE DON'T JUST RUN TESTS—WE UNCOVER WHAT OTHERS MISS. OUR OFFENSIVE SECURITY TEAM THRIVES ON RESEARCH, INNOVATION, AND DELIVERING REAL VALUE THROUGH CRITICAL VULNERABILITY DISCOVERY.

REDINGTON MEA DRIVES REGIONAL PUSH TO DEMOCRATISE CYBERSECURITY

SAYANTAN DEV, PRESIDENT, MEA, REDINGTON, SPOKE WITH CPI MEDIA AT GISEC 2025 ABOUT SECURITY PREDICTIONS FOR THE COMING YEAR AND HOW THEY ARE LEVERAGING NEW TECHNOLOGIES TO SUPPORT PROACTIVE THREAT DETECTION.

Cyber threats are becoming more advanced, and the expanding digital footprint of enterprises is creating new vulnerabilities across hybrid and multi-cloud environments. From AI-powered phishing attacks to surging ransomware incidents, businesses in the Middle East are under constant pressure to defend an ever-shifting attack surface. Meeting this challenge requires a proactive, collaborative, and scalable approach to cybersecurity.

Redington MEA is driving this transformation by helping organisations of all sizes access next-generation security solutions. Speaking to CPI Media Group at GISEC 2025, Sayantan Dev, President – MEA at Redington, outlined the company's strategy for strengthening cyber resilience through AI integration, cross-sector collaboration, and regional compliance readiness.

What emerging cybersecurity threats or trends do you believe will most significantly impact enterprises in the Middle East and beyond in the coming year?

We're seeing a big rise in ransomware, supply chain attacks, and sophisticated phishing campaigns — and they're only getting smarter with the use of AI. According to some reports, ransomware attacks globally jumped over 50% last year, and the Middle East is no exception. Another key trend is the attack surface getting bigger as businesses go hybrid, with people, devices, and data spread across cloud, edge, and on-prem environments. So, the challenge isn't just to protect systems — it's to protect a constantly moving target.

You can't prevent everything — so, prevent what you can, detect what you can't prevent, and hunt what you can't detect.

How is your company collaborating with governments or enterprises to strengthen cyber resilience across sectors?

At Redington, we work closely with both governments and enterprises to strengthen cyber resilience across the region.

By leveraging AI, organisations can build more resilient cybersecurity postures, better equipped to withstand

and recover from cyberattacks.

Through our MSSP practice, DigiGlass, and partnerships with top global vendors, we provide organisations with comprehensive visibility across their infrastructure through a single pane of glass, coupled with high-level MDR capabilities, ensuring compliance with regional data-handling requirements tailored to specific industry verticals. Cyber resilience goes beyond just people, processes, and technology. A critical element is the threat intelligence that powers stronger detection capabilities. We've integrated multiple threat intelligence platforms and are actively collaborating with the UAE Cybersecurity Council to gain comprehensive visibility into regional threat dynamics. This collaboration ensures our solutions are fully compliant with regional standards like DESC, enabling us to provide our customers with maximum protection.

What message would you like to share with the global infosec community attending GISEC about your vision for cybersecurity in 2025 and beyond?

Our message is clear: cybersecurity is no longer just an IT issue; it's a business

**TOGETHER WITH OUR
PARTNERS, WE AIM
TO DEMOCRATISE
CYBERSECURITY AND
MAKE IT ACCESSIBLE,
SCALABLE, AND EFFECTIVE
ACROSS THE REGION.**

Sayantana Dev
President, MEA, Redington.

enabler. We believe the future of security is all about being proactive, data-driven, and collaborative. At Redington, our focus is on helping businesses of all sizes access cutting-edge solutions, close the skills gap, and build resilience that keeps up with innovation. Together with our partners, we aim to democratise cybersecurity and make it accessible, scalable, and effective across the region.

How is Redington MEA leveraging new technologies like AI and machine learning to enhance cybersecurity solutions and support proactive threat detection?

We're already integrating AI and

machine learning into many of our offerings, particularly through our MXDR solution powered by Microsoft Sentinel and Defender. AI helps us detect threats faster, cut down on false alarms, and even predict attacks before they hit. For example, we've seen a 30–40% improvement in detection speed in some deployments. With these technologies, our teams and partners can spend less time reacting — and more time strengthening defences.

With the increasing demand for hybrid and multi-cloud environments, how is Redington MEA helping businesses ensure security and scalability

while adopting these complex architectures?

Hybrid and multi-cloud setups bring great flexibility but also more complexity and risk. At Redington, we help businesses navigate this with solutions that are cloud-native, scalable, and easy to integrate — whether that's through our AWS Marketplace Practice, Microsoft cloud portfolio, or security practices like DigiGlass. We also work closely with customers through our channel partners to design architectures that balance performance and protection, so they can grow with confidence without compromising security. 🔑

REDINGTON SHAPES FUTURE OF CLOUD AND CYBERSECURITY IN MIDDLE EAST

NEHAL SHARMA, VICE PRESIDENT OF CLOUD SOLUTIONS AT REDINGTON, SPOKE TO SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP, ABOUT THE COMPANY'S ROLE IN DRIVING REGIONAL DIGITAL INITIATIVES, CLOUD ADOPTION, AND OVERCOMING KEY CHALLENGES AT GISEC GLOBAL 2024.

Redington plays a pivotal role in shaping the cloud and cybersecurity landscape in the Middle East and Africa. At GISEC Global 2024, Nehal Sharma, Vice President - Cloud Solutions Group at Redington, discussed the company's approach to empowering partners, driving innovation, and addressing key challenges in the ever-evolving industry. In this exclusive interview, Nehal highlights Redington's strategies for cloud technologies, cybersecurity, and its transformative role in the region.

How does Redington's presence at GISEC Global align with your broader cybersecurity strategy for the region?

From Redington's perspective, we aim to be a comprehensive aggregator for our channel. Our goal is to create an ecosystem that empowers our partners to explore new opportunities. At GISEC,

there's a lot to discover—new names, new ideas—and it's exciting to see the level of preparedness from our key players. For us, cybersecurity is a combination of technology, policies, and practices. Redington's role is to bring these elements together to ensure that security is viewed as everyone's problem, not just a single person's responsibility.

Can you highlight any innovative technologies or solutions Redington showcased at GISEC West?

We showcased several technologies from our key partners like Norman Tech, IDC Technologies, and Expedite. These partners have been crucial in driving perspectives for customers and helping them establish proper security measures. We've also developed an asset through our Microsoft managed services security practices. This asset is designed to democratise security for our channel, ensuring that solutions are maximised



REDINGTON IS KEEN TO ADDRESS THE REGIONAL SKILLS GAP BY DRIVING PRACTICES THAT HELP BUSINESSES LEVERAGE CLOUD EFFECTIVELY AND MULTIPLY THEIR IMPACT THROUGH THE RIGHT PARTNERSHIPS.



Nehal Sharma
Vice-President of Cloud
Solutions at Redington.

for customers without requiring large investments upfront. It's about guiding customers through the entire journey, not just selling them a product.

How do you see the role of cloud technologies in transforming businesses across the Middle East and Africa, especially in the context of regional digital transformation initiatives?

The Middle East and Africa is a vast and diverse region. Within the Middle East, countries like the UAE and Saudi Arabia are leading the charge in digital transformation. Cloud has evolved from a

mere infrastructure tool to a fundamental component of every business strategy. In the past, cloud was seen as a phenomenon; today, it's the foundation for nearly everything—from security to AI, SaaS, and more. Redington is keen to address the regional skills gap by driving practices that help businesses leverage cloud effectively and multiply their impact through the right partnerships.

What challenges do businesses face when adopting cloud solutions in this region, and how does Redington help overcome them?

Cloud adoption involves various pillars such as infrastructure, security, data, AI, and intelligence. Each customer's journey is different, which can make it difficult to align all of these elements. We've created specialised practices to address these challenges—whether it's through data, migration, SAP, or security practices. Our approach is that if a customer faces a problem, it becomes our problem too. We aim to help businesses build strong fundamentals that support AI adoption and ensure the successful integration of cloud technologies into their operations. 🌱

RESECURITY AND STARLINK QATAR INK STRATEGIC CYBERSECURITY PARTNERSHIP

IMPOWERING
THE META REGION
WITH NEXT-GEN
CYBER RESILIENCE
THROUGH A
POWERFUL
ALLIANCE.

Resecurity, a global cybersecurity leader, has partnered with Starlink to expand advanced threat protection across the region. A subsidiary of Ooredoo Group, Starlink has more than 18 years of experience in Qatar's ICT and mobile accessories market. Starlink's ICT Distribution focus areas include cybersecurity, cloud, datacenter, AI, networking and physical security. This partnership brings together deep expertise and innovation to deliver tailored, future-ready security solutions for today's evolving digital challenges.

Through this partnership, Resecurity's cutting-edge cybersecurity solutions will be integrated into Starlink's extensive distribution network, enabling organisations across the META region to proactively detect, analyse, and respond to cyberthreats. The collaboration focuses on delivering technologies and services that enhance digital resilience and protect against evolving cyberthreats.

"Our partnership with Starlink represents a significant step in our mission to provide advanced



**Cyril Anand, CEO of Starlink Qatar
and Ahmad Halabi, Managing
Director, Resecurity Inc.**

cybersecurity solutions across the META region,” said Gene Yoo, CEO of Resecurity. “By combining our expertise with Starlink’s extensive regional presence, we aim to empower organisations to proactively address cyberthreats and enhance their security posture.”

“Collaborating with Resecurity allows us to expand our cybersecurity portfolio and offer our clients innovative solutions that address the dynamic threat landscape,” said Cyril Anand, CEO of Starlink Qatar. “Together, we are committed to delivering technologies that not only protect but also empower

businesses to thrive in a secure digital environment.”

The partnership was officially announced during GISEC Global 2025, the region’s premier cybersecurity event held at the Dubai World Trade Centre, serving as a launch platform for strategic cybersecurity collaborations. 🔒



**TOGETHER, WE ARE
COMMITTED TO DELIVERING
TECHNOLOGIES THAT NOT ONLY
PROTECT BUT ALSO EMPOWER
BUSINESSES TO THRIVE IN A
SECURE DIGITAL ENVIRONMENT
CYRIL ANAND, CEO OF STARLINK
QATAR**

UAE TAKES LEAD IN AI-DRIVEN DIGITAL TRANSFORMATION WITH DYNATRACE'S OBSERVABILITY VISION

PHILIPPE DEBLOIS, GLOBAL VP, SOLUTIONS ENGINEERING AT DYNATRACE, DISCUSSES THE UAE'S DIGITAL EDGE, THE EVOLUTION OF OBSERVABILITY, AND HOW AI IS SHAPING THE FUTURE OF IT OPERATIONS.

With the UAE fast emerging as a global hub for digital innovation and AI integration, industry leaders are keenly investing in solutions that simplify complexity and drive performance across hybrid cloud environments. Dynatrace, a global leader in Observability, is among the few vendors making deep inroads in the region by enabling enterprises to anticipate, automate, and accelerate their digital journeys. In this exclusive conversation, Philippe Deblois, Global Vice President, Solutions Engineering at Dynatrace, shared his top insights with Sandhya D'Mello, Technology Editor, CPI Media Group, on why the UAE is a magnet for next-gen digital projects, how Observability is evolving into a

business-critical strategy, and why AI isn't just a feature—but the foundation of the future.

Where do you see the UAE in terms of its digital transformation journey? What stands out to you most?

The UAE is currently one of the most exciting places for digital transformation. There are numerous ongoing projects, and partnerships such as NVIDIA with G42 and Humane in Saudi Arabia are advancing the concept of AI factories. The Emirates are clearly leading this movement. At Dynatrace, we've seen this as a reason to significantly expand our presence—investing in resources, growing our team by 280%, and launching our own cloud instance in Abu Dhabi. We are the only Observability vendor to do so.

How is Observability evolving from traditional monitoring to a full-scale business solution?

Traditional monitoring was reactive: a problem occurs, then you respond. Observability, on the other hand, is proactive. It helps prevent issues before they arise by enabling automation, auto-remediation, and performance optimisation. It spans across multi-cloud and hybrid environments and even integrates with AI agents—creating a comprehensive solution that supports modern digital systems.

Can you explain Observability in simple terms?

Observability is essentially about visibility—understanding how systems perform and interact. It's designed to work across all systems, helping

identify performance gaps and enabling automated optimisation and protection.

What makes Dynatrace's Observability platform unique in today's complex IT environments?

What sets Dynatrace apart is our all-in-one platform approach. We developed our own backend architecture called Grail, which consolidates logs, traces, metrics, and business/security events into a single data layer. Additionally, AI is built into the core—not added on. We use what we call the “power of three”: causal AI, predictive AI, and generative AI. We're also exploring agentic AI for orchestrated communication between AI agents and systems.

Does managing such AI-powered systems require specialised manpower? Are users equipped to handle this?

There's a global need to upskill for AI, no doubt. But with Dynatrace, users don't need to be AI experts. Our platform handles the complexity behind the scenes. Users only need to learn how to apply the insights to improve customer or business outcomes.

Do you encounter resistance from traditional mindsets when advocating for Observability and cloud adoption?

Yes, we often do. While innovators grasp the need, some laggards still hesitate. But as businesses move away from three-tier applications toward microservices and cloud-native models, complexity increases. That's when they start seeing value in Observability—especially when it helps them reduce



Philippe Deblois, Global VP, Solutions Engineering at Dynatrace.

friction and gain control during transformation.

Which industries in the UAE are adopting Observability solutions most rapidly?

We've seen strong adoption in government, banking, and aviation. These sectors rely heavily on customer-facing applications, and any disruption

directly impacts user experience. Companies are prioritising performance because customers today are vocal—especially on social media—and poor experience can harm reputation fast.

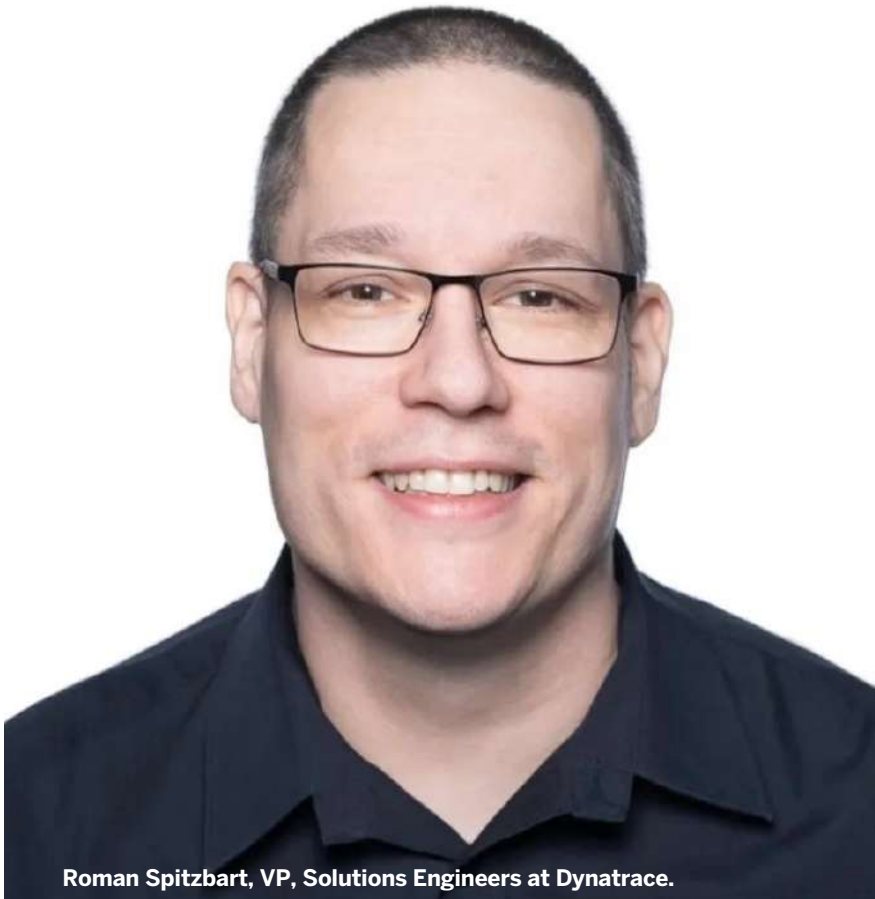
What are your top tips for businesses aiming to stay competitive and resilient through Observability?

First, treat Observability as essential—not optional. Modern IT environments are too complex to manage without it. Second, use Observability to enhance security—identify vulnerabilities and prioritise fixes. Third, focus on business Observability—understanding critical processes like account openings in banking can reveal operational inefficiencies and help improve customer satisfaction. 📌

“WE USE WHAT WE CALL THE “POWER OF THREE”: CAUSAL AI, PREDICTIVE AI, AND GENERATIVE AI. WE’RE ALSO EXPLORING AGENTIC AI FOR ORCHESTRATED COMMUNICATION BETWEEN AI AGENTS AND SYSTEMS.”

DYNATRACE DRIVES REAL-TIME AI GOVERNANCE, DATA SOVEREIGNTY IN ENTERPRISE LANDSCAPE

ROMAN SPITZBART, VP, SOLUTIONS ENGINEERS AT DYNATRACE, SHARES INSIGHTS WITH SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP ON HOW THE COMPANY IS CHAMPIONING REAL-TIME OBSERVABILITY, SECURE DATA GOVERNANCE, AND AI-POWERED AUTOMATION TO SUPPORT TRANSPARENCY AND TRUST ACROSS REGULATED INDUSTRIES.



Roman Spitzbart, VP, Solutions Engineers at Dynatrace.

How is Dynatrace positioning itself to lead conversations around transparent and responsible AI governance in the enterprise space?

Responsible AI governance begins with real-time visibility. It's not enough to identify issues after the damage is done. Dynatrace integrates observability into AI applications from day one, ensuring organisations can track, govern, and secure usage as it happens. In a climate where AI adoption often outruns regulatory readiness, Dynatrace helps enterprises maintain control, transparency, and due diligence.

How does Dynatrace's Grail engine support traceability and explainability of AI models, particularly in regulated industries like banking and finance?

Grail provides deep visibility into every step of a transaction, including the AI layer—whether that's a language model



or inference engine. This aligns with our core approach of tracking end-user interactions across complex applications. In regulated industries, the focus is on preventing data intermingling. Dynatrace ensures that all AI interactions are contextually bound to each customer's data, maintaining strict isolation to safeguard compliance.

With growing concerns about data privacy and compliance, how does Dynatrace ensure long-term data security and audit-readiness while maintaining rapid querying capabilities?

Our unified storage architecture eliminates the need to move data between hot and cold layers, which can compromise access controls. This design keeps data instantly accessible while retaining all security parameters. We rely on hyperscalers like AWS, Azure, and GCP for storage but enforce granular, built-in access controls. Every action is authenticated based on user

rights, ensuring audit readiness and robust compliance without performance trade-offs.

How is the intersection of observability and AI governance evolving, and what role will Dynatrace play in this future?

AI governance is accelerating innovation, and observability must keep pace. Dynatrace is embedding automation and AI observability into the application

WE AIM TO HELP ORGANISATIONS MONITOR AND OPTIMISE AI USE AT SCALE—WITHOUT COMPROMISING COMPLIANCE OR BUDGET.

lifecycle to ensure issues are preemptively managed. Our platform supports secure, cost-efficient deployment of AI systems by ensuring visibility isn't an afterthought. We aim to help organisations monitor and optimise AI use at scale—without compromising compliance or budget.

Given Dynatrace's global footprint and access to sector-specific data, how do you ensure data sovereignty while enabling advanced insights like demand forecasting?

Data is an enterprise's most valuable resource, but we treat it as our customer's property. Dynatrace does not access or analyse customer data without explicit approval. Any such access follows a strict audit trail and customer-controlled process. Even as a SaaS provider, we do not bypass this. We ensure full data segregation and transparency, reinforcing trust in our role as a custodian, not an owner, of enterprise data. 📌



Edgard Capdevielle
CEO of Nozomi Networks.

NOZOMI STRENGTHENS GLOBAL AND REGIONAL DEFENSES AGAINST RISING INFRASTRUCTURE CYBER THREATS

EDGARD CAPDEVIELLE, CEO OF NOZOMI NETWORKS, SHARES PRESSING GLOBAL AND REGIONAL INSIGHTS ON THE EVOLUTION OF CYBER THREATS, AI'S DUAL ROLE IN DEFENSE AND OFFENSE, AND THE URGENT NEED TO SECURE OPERATIONAL TECHNOLOGIES ACROSS SECTORS, WITH SANDHYA D'MELLO, TECHNOLOGY EDITOR, CPI MEDIA GROUP.

→ **AI HELPS MITIGATE THESE RISKS BY ENHANCING REAL-TIME MONITORING, PREDICTIVE ANALYTICS, AND ADAPTIVE THREAT RESPONSE ACROSS SECTORS INCLUDING ENERGY, TOURISM, AND MANUFACTURING.**

What has been the most significant shift in cyber threats targeting critical infrastructure globally over the past 12 to 18 months, and how has AI evolved in both offensive and defensive strategies?

Cyber threats targeting critical infrastructure have become increasingly sophisticated and relentless. Global tensions and geopolitical conflicts often coincide with a surge in cyber activity—ransomware, for example, has grown rampant. AI plays a central role in both attack and defense. Threat actors leverage AI for reconnaissance, social engineering, and code development,

while defenders are integrating AI to detect anomalies, enhance visibility, and respond to threats. At Nozomi Networks, our entire platform was built at the intersection of AI and OT security, enabling advanced protection for industrial systems.

What advanced attack tactics are you observing, and how can infrastructure operators defend against these emerging threats?

One major development is the increasing exploitation of the wireless attack surface, particularly in OT and IoT environments. Attackers can now access systems remotely, even from outside facilities like parking lots. Additionally, “living off the land” attacks—where threat actors exploit legitimate system tools—are hard to detect. Criminals and nation-state actors use AI to craft zero-day exploits and personalized phishing attempts. To counter these threats, we’ve introduced wireless sensors to broaden visibility and defense.

What are the top three emerging threats that critical infrastructure operators need to prepare for, and how can AI help mitigate these risks?

- 1. Ransomware:** It has leveled the playing field, making even non-financial sectors prime targets.
- 2. Wireless Attacks:** Wireless infrastructure can now be exploited externally, bypassing traditional firewall defenses.
- 3. AI-driven Threats:** AI enables highly targeted and automated attacks.

AI helps mitigate these risks by enhancing real-time monitoring, predictive analytics, and adaptive threat response across sectors including energy, tourism, and manufacturing.

How have regional challenges in the Middle East and Africa impacted the cybersecurity posture of critical

infrastructure? Are there specific sectors at heightened risk?

The GCC region’s dependence on critical sectors like oil, gas, water, and energy, combined with ongoing digital transformation and IT-OT convergence, has expanded the attack surface. There’s an influx of both cyber criminals and nation-state actors. While the region is advancing in cybersecurity maturity, challenges persist due to legacy OT systems interacting with modern IT, often with inadequate protection.

What role do regional regulations and cybersecurity frameworks play in securing critical infrastructure, and how can these be improved?

Regulatory bodies across the GCC are becoming more proactive. The UAE’s National Cybersecurity Strategy and Saudi Arabia’s ECC framework under the NCA are setting foundational standards. Cross-country cooperation is also growing. However, regulations should go beyond compliance and push for proactive risk management. The focus must shift from incident response to predictive protection, supported by a shared risk language across sectors.

Is there a gap between the sophistication of cyber threats and the preparedness of critical infrastructure operators in this region? How can this gap be addressed?

For years, financial and retail industries evolved in lockstep with cybercriminals, while critical infrastructure lagged behind. Operators now face nation-state-grade threats without the legacy of security investment or practices. Bridging this gap requires not just technical upgrades but cultural and budgetary shifts—security must become embedded into every layer of operations. 🔑

THE CRITICAL IMPERATIVE OF HEALTHCARE CYBERSECURITY

EVEN LIFE-SAVING TECHNOLOGY CAN BECOME LIFE THREATENING AS MODERN HEALTHCARE FACILITIES ARE FACING INCREASING ATTACKS FROM CYBER CRIMINALS.

In February 2024, a ransomware attack on Change Healthcare devastated healthcare systems across the USA, with patients unable to access vital treatments. Essential clinical and eligibility services collapsed, and healthcare providers across the country faced potential financial ruin.

Such scenarios are the growing reality of cybersecurity threats in modern healthcare.

As medical facilities increasingly rely on interconnected devices and digital systems, a new frontier of vulnerability has been created. The critical intersection of healthcare delivery and digital security demands urgent attention, as healthcare institutions worldwide race to protect their most vital assets: patient data, medical devices, and ultimately, human lives.

Key challenges

The fundamental lack of understanding regarding the unique cybersecurity risks inherent in healthcare is a key challenge. Many large healthcare organizations lack complete visibility into the assets and systems connected to their networks. Without a comprehensive inventory of these assets, that can often amount to tens of thousands in major hospitals, it is extremely difficult to implement effective security measures.

A critical first step is increasing awareness about specific technologies and protocols deployed within healthcare institutions, including both IT and

operational technologies, many of which play a vital role in patient care but are often overlooked in traditional cybersecurity strategies.

Healthcare services are critical and protecting them requires a strategic, well-coordinated approach, combining asset visibility, protocol awareness, regulatory alignment, and a strong cybersecurity foundation. Around the world, governments and regulatory bodies are increasingly introducing tailored governance models to strengthen cybersecurity within healthcare, driven by heightened risks as medical IoT (Internet of Things) devices become more prevalent.

The new frontiers of vulnerability

Hospitals are integrating a wide range of smart, connected systems—from heart monitors and lung pumps to blood purification machines and diagnostic tools. Historically, these systems were operated offline, but today, they are increasingly online to enable real-time data access and improved clinical decision-making.

The increased adoption of Operational Technology (OT) and Internet of Things (IoT) devices has enhanced patient care, improved efficiency, and helped healthcare become more competitive and responsive.

However, this connectivity poses new risks. As the larger, interconnected ecosystem grows, so does the attack surface, providing cyber adversaries with more potential entry points.

Moreover, many medical devices lack the memory or processing capabilities to support traditional security controls such as antivirus software or encryption.

To address this, cybersecurity experts focus on network-level visibility and segmentation, along with specialized protocols for medical environments. These strategies aim to identify assets, understand vulnerabilities, and apply controls at the network layer rather than relying on the devices themselves.

AI and ML in Cybersecurity

Emerging technologies—particularly artificial intelligence and machine learning—are increasingly critical to

HEALTHCARE SERVICES ARE CRITICAL AND PROTECTING THEM REQUIRES A STRATEGIC, WELL-COORDINATED APPROACH, COMBINING ASSET VISIBILITY, PROTOCOL AWARENESS, REGULATORY ALIGNMENT, AND A STRONG CYBERSECURITY FOUNDATION.



**Nikola Kukoljac, Vice President
Solution Architecture, Help AG.**

strengthening cybersecurity within healthcare environments.

AI-powered platforms can automatically identify all connected devices within a healthcare network, including those that may not have been manually logged or traditionally monitored—a crucial first step in understanding what needs to be protected.

AI and ML can also identify vulnerabilities and detect threats in real time, analyzing vast amounts of network activity and system behavior to recognize a potential cyberattack—far quicker than manual methods.

AI can also prioritize risks, so healthcare IT teams focus on the most critical threats first, which is essential in the fast-paced nature of medical environments where resources are often stretched thin.

While foundational practices like cyber hygiene—regular patching, updates, and system maintenance—remain essential,

AI and ML provide an intelligent layer that enhances an organization's ability to predict, detect, and respond to threats more effectively.

As threats evolve, the integration of AI-driven tools, alongside adherence to regulatory compliance and governance standards, positions healthcare institutions to be more resilient, secure, and future-ready.

How to protect medical data

Protecting medical data is fundamentally no different from safeguarding other forms of personal data, as it adheres to the core principles of cybersecurity.

Firstly, strong passwords or biometric authentication for any connected health devices or applications are recommended to safeguard sensitive medical information from unauthorized access.

Secondly, personal medical information should only be shared with trusted healthcare providers, institutions,

or entities, ensuring they adhere to appropriate security and privacy standards.

Lastly, medical data should be stored in secure environments that follow stringent protocols for encryption and access control. Data must be properly destroyed once it's not required to prevent any potential exposure.


As healthcare systems evolve and more data is digitized, maintaining sound cybersecurity habits is essential for both personal and public health protection.

The Abu Dhabi Model

The 2025 edition of Abu Dhabi Global Health Week demonstrated how the UAE is shaping the global health agenda by enabling collaboration and innovation, while addressing the world's most urgent health challenges.

Recognizing early on that technological adoption must complement strong cybersecurity governance, the UAE implemented a well-defined legislative framework to protect healthcare systems – emphasizing integrating international cybersecurity standards into local practices.

In February 2019, the President of the UAE issued Federal Law No 2 of 2019 (Health Data Law), directly addressing healthcare data protection. The Health Authority of Abu Dhabi (HAAD) ensures the confidentiality, integrity, and availability of healthcare information through clearly outlined protocols set out in The Abu Dhabi Healthcare Information and Cybersecurity Standard. Aligning the healthcare sector with cybersecurity best practices, Abu Dhabi is thus fostering cyber resilience, enabling safe and secure healthcare delivery.

From Abu Dhabi to worldwide healthcare systems, there's growing recognition that digital transformation in healthcare can only succeed when built upon a foundation of robust security. The integrity of our most personal data, and even our physical well-being, depends on our collective commitment to this cause. 

UIPATH APPOINTS SARA AL-ALSHEIKH AS REGIONAL VICE PRESIDENT FOR SAUDI ARABIA

THE COMPANY'S FIRST FEMALE LEADER IN SAUDI ARABIA, KUWAIT, AND BAHRAIN BRINGS OVER A DECADE OF TECH LEADERSHIP TO DRIVE CUSTOMER SUCCESS AND REGIONAL GROWTH



UiPath (NYSE: PATH), a global leader in agentic automation, announced the appointment of Sara Al-Alsheikh as Regional Vice President (RVP) and Managing Director for Saudi Arabia, Kuwait, and Bahrain, amid rising demand for AI-powered automation adoption across the Gulf.

Based in Riyadh, Al-Alsheikh will lead UiPath's go-to-market and customer success strategy across Saudi Arabia, Kuwait, and Bahrain and act as Managing Director of the UiPath regional hub, headquartered in Riyadh. Al-Alsheikh will focus on accelerating growth in key sectors such as government, banking, oil and gas, and others, strengthening UiPath's partner ecosystem, and driving customer success across large-scale digital transformation initiatives.

Agentic Automation Momentum Across the Gulf

The Gulf region is experiencing a significant surge in digital transformation initiatives, with organizations increasingly adopting advanced automation technologies to enhance efficiency and competitiveness. UiPath is at the forefront of this evolution, enabling local businesses and governments to develop and orchestrate complex AI-powered automation deployments through seamless integration of AI agents, software robots, and human collaboration.

Thanks to her exceptional track record of proven success having worked closely with UiPath customers in the region since joining in 2023 as Director of Public Sector and Public Investment Fund (PIF), Al-Alsheikh's appointment aligns with this momentum. Furthermore, it

is placing UiPath in a solid position to further support the Gulf's ambitious Vision 2030 objectives by fostering innovation and driving sustainable growth across key sectors, while also supporting gender inclusion goals.

Sara's appointment reflects the Kingdom's ongoing transformation and growing emphasis on empowering women in leadership as part of Vision 2030. With over a decade of experience at global technology firms including HP, IBM, and SAP, she represents a new generation of Saudi leaders driving innovation, inclusion, and sustainable growth across the region's technology landscape.

"I could not be more thrilled to step into this leadership role at such a pivotal time when the Kingdom is accelerating its digital transformation roadmap and making AI a cornerstone of its strategy. At the same time, UiPath has reached a pinnacle of innovation through the recent relaunch of the UiPath Platform as the first enterprise-grade platform for agentic automation on the market" said Sara Al-Alsheikh, Regional Vice President and Managing Director for Saudi Arabia, Kuwait, and Bahrain at UiPath. "My mission is to help our clients reimagine how work gets done faster, smarter, and more autonomously thanks to agentic automation, with UiPath at the core of their innovation journey."

"Sara's leadership is a strategic asset for UiPath and a symbol of what's possible when talent, vision, and inclusion intersect," said Zakaria Haltout, Area Vice President Middle East and Africa at UiPath. "She brings not only invaluable regional insight but also the drive to execute at scale, and we are excited to see her lead our next chapter of growth." 🗣️



CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD
CLEANROOM™ RECOVERY



Commvault®

Visit commvault.com to Learn More



Sean Malone

BEYONDTRUST NAMES INDUSTRY VETERAN SEAN MALONE AS CHIEF INFORMATION SECURITY OFFICER

BeyondTrust, the global cybersecurity leader protecting Paths to Privilege, has announced Sean Malone as its new Chief Information Security Officer (CISO). With 15+ years of experience and proven

leadership in the cybersecurity industry, Malone will oversee BeyondTrust's global security strategy, including security for products and services, threat management, cyber risk and compliance, and security operations.

With a career spanning offensive

- Experienced security leader joins BeyondTrust to drive innovation and strengthen identity security leadership
- Sean Malone brings deep expertise in offensive security, cyber risk, and threat management to CISO role

security, cyber risk quantification, and executive leadership, Sean Malone brings a unique blend of hands-on technical expertise and strategic vision to the CISO role. At Demandbase, as CISO, he led global security operations, influenced R&D strategy, and regularly advised executive leadership on risk governance. His experience at Amazon Prime Video strengthened enterprise cyber defense at scale, while his leadership at VisibleRisk and BitSight honed his ability to quantify and communicate cyber risk. As a U.S. patent holder for "Systems and Methods for Assessment of Cyber Resilience," Sean has consistently driven security innovation, making him exceptionally well-equipped to lead BeyondTrust's security strategy.

"I am thrilled to welcome Sean to the BeyondTrust security team," said Janine Seebeck, CEO at BeyondTrust. "As we continue to grow the company and advance our mission of helping customers solve their real-world security problems, Sean's leadership will be instrumental in ensuring BeyondTrust sets the standard for security excellence."

"I spent the first decade of my career on the offensive side, acting as a simulated adversary in red team engagements to challenge large companies facing constant threats," said Sean Malone, CISO at BeyondTrust. "Having seen firsthand that nearly every successful cyberattack exploits an unnecessary path to privilege, I'm excited to lead security at BeyondTrust. Security is not just central to BeyondTrust's mission—BeyondTrust is essential to the broader security mission for the industry as a whole." 🦋



Securing identities at every interaction

Seamless, intelligent, centralized authorization to better secure the modern enterprise



Secure Credentials



Privileged Remote Access



Privilege & Entitlement Elevation



Identity Threat Protection



Identity Governance



Follow us on



delinea.com



Smart Monitoring Solutions

Free Lifetime Video Recording

3 Year Warranty

Free Installation

Free after-sales service

Keep an eye on your home even when you are away

With Ring Video Doorbells and Security Cameras, you can monitor every corner of your property.

Starts at AED 20*

