

Security

ADVISOR

MIDDLE EAST



FROM SKILLS GAP TO SECURITY POWERHOUSE

HOW SANS INSTITUTE AND NED BALTAGI ARE TRANSFORMING
REGIONAL TALENT INTO FRONTLINE DEFENDERS OF THE DIGITAL AGE.



ISACA
UAE Chapter

&
tahawultech.com
presents

INFOSEC & CYBERSECURITY CONGRESS 2025

Securing the Intelligent Age

📅 18th June 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 **18th June 2025** at **VOGO Abu Dhabi Golf Resort & Spa**,
and be part of the movement shaping the future of secure digital transformation.

GOLD SPONSORS

Delinea
Securing identities at every interaction

HPE **aruba**
networking

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



6

Cyber First Kuwait returns to drive national cyber resilience aligned with Vision 2035

32

OPSWAT announces GISEC 2025 participation with a focus on critical infrastructure

18

Fujairah ignites tech future with Young Techpreneurs initiative

34

Fortinet strengthens AI-powered cybersecurity vision at GISEC Global 2025



21 – 23
MAY 2025
MESSE BERLIN
— SOUTH ENTRANCE —

FEATURING



Germany's Largest Tech, Startup & Digital Investment Event

2,000+
EXHIBITORS

1,000+
STARTUPS

800+
INVESTORS

100+
COUNTRIES

ENDORSED BY



GET INVOLVED



#GITEXEUROPE
gitex-europe.com

EDITOR'S NOTE



Talk to us:
E-mail:
sandhya.dmello@cpimediagroup.com

Sandhya DMello
Editor

SHAPING THE FUTURE OF CYBERSECURITY THROUGH TALENT AND INNOVATION

The future of cybersecurity is being shaped not just by technologies, but by the people who wield them. This issue shines a light on the bold efforts of Ned Baltagi and the SANS Institute, who are working tirelessly to build a strong, self-sufficient cybersecurity workforce across the Middle East and Africa. By bridging education, industry, and innovation, they are nurturing the next generation of defenders who will stand at the frontline of a constantly evolving digital world.

Across the region, momentum is building.

Emirates NBD's adoption of Kinexys Liink signals a commitment to more secure cross-border payments. SentinelOne's recognition for excellence, Cyber First Kuwait's focus on national cyber strength, and SandboxAQ's new platform to secure AI-driven environments reflect the growing sophistication in cybersecurity responses. The innovation landscape continues to

expand with Veeam fortifying identity resilience, Cohesity advancing quantum-proof encryption, and HID redefining security integration for the digital age.

This edition also brings a special spotlight on the exclusive conversation with Dr Ahmed Hamdan Al Zeyoudi from Fujairah's Young Techpreneurs initiative, offering a glimpse into how future generations are being empowered with skills in AI, coding, and cybersecurity. Our extensive coverage of

GISEC Global 2025 captures the energy of one of the region's most influential security gatherings, where

global thought leaders are driving the dialogue on AI-powered security strategies, critical infrastructure protection, and exposure management.

Security Advisor Middle East remains committed to celebrating the individuals, institutions, and innovations shaping a safer, smarter, and more resilient digital future.

EMPOWERING CHANGE, ENABLING FUTURE

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
Prajith Payyapilly
prajith.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.

CYBER FIRST KUWAIT RETURNS TO DRIVE NATIONAL CYBER RESILIENCE ALIGNED WITH VISION 2035

Conference unites leaders from government and industry to explore Kuwait's ambitious cybersecurity transformation

In a time of accelerating digital

transformation, the 3rd Cyber First Kuwait Edition took center stage at the Radisson Blu Hotel, Kuwait, bringing together over 300 technology leaders, cybersecurity professionals, and policymakers to address the country's evolving digital threat landscape and cybersecurity vision. Organized by Events First Group, the conference supports the new Kuwait Vision 2035 and the nation's ambitious National Cybersecurity Strategy.

The summit featured keynote presentations, expert panel discussions, real-world case studies, and an exhibition showcasing cutting-edge solutions. Topics included AI-powered threat detection, OT/ICS infrastructure security, cloud resilience, Zero Trust frameworks, and national-level collaboration between public and private sectors.

Abdullah Al Shaheen, Director of Public Relations and Media Department at National cybersecurity center said, "This edition of the Cyber First Conference, held under the patronage of the National Cybersecurity Center serves as a platform for business



Mohamed El-Demery, Cybersecurity Consultant, Confidential; Faissal Al Roumi, Head Operational Risk, Burgan Bank; Dr. Shaheela B Abdul Majeed, Information Security and Compliance Officer, Oil and Gas Industry; Dr. Sulaiman Alhasawi, Founder of ICS Arabia Podcast and ICSRANK; Nicholas Palmer, Head of Business Development & Sales, Group-IB; Abdullah AlSabah, Head of International Relations, Ministry of Defence; and Ali Waleed Saleh Alqallaf, Head of Project, Security Operations, Kuwait National Petroleum Company (KNPC).

leaders, professionals to come together and exchange experiences, share best practices, and explore the latest developments for security and protection against the rapidly evolving cyber threats and attacks. These challenges require us to remain informed and constantly evolving."

"The National Cybersecurity Center in the State of Kuwait is working to build an effective system to protect the cyberspace by collaborating with both

local and international entities in the field of cybersecurity. This is to create a safe digital environment, while maintaining the trust of technology operators and users. We hope this conference will serve as a gateway to more important meetings and events that focus on cybersecurity," he added.

"Cyber First Kuwait is a national dialogue and strategic catalyst," said Shyam Reddy, Partnerships Director. "With Vision 2035 and the National Cybersecurity Strategy serving as our guiding frameworks, this summit brings together government and enterprise to create actionable pathways toward a digitally secure and resilient Kuwait."

The conference featured keynotes, panels, one-on-one networking sessions, a cybersecurity hackathon, and the Kuwait Cybersecurity Awards, recognizing trailblazers across innovation, leadership, and operational excellence.

The event hosted over 300 delegates, including CISOs, risk management leaders, OT and cloud architects, regulators, leading solution providers, more than 20 sponsors, 15 media partners, and 10 ministries.



Lt. Colonel Eng. Mohammad Alawadhi, Head of Information Security, Kuwait Fire Force; Colonel Eng. Aqeel Aljadi, Cybersecurity Supervisor, Kuwait Fire Force; Abdullah Al Shaheen, Director of Public Relations and Media, National Cyber Security Center; and Shyam Reddy, Strategic Partnerships Lead, Events First Group.

EMIRATES NBD'S COLLABORATION WITH KINEXYS TO ENHANCE CROSS-BORDER PAYMENT SECURITY

Emirates NBD joins Kinexys Liink to pioneer blockchain-powered cross-border payment validation and security in the MENAT region.



Emirates NBD a leading banking group in the Middle East, North Africa, and Türkiye (MENAT) region, announced its strategic decision to join Kinexys Liink, the world's first bank-led peer-to-peer data sharing network, from Kinexys by J.P. Morgan. Through integrating with Kinexys Liink's 'Confirm' Application, designed for the exchange of global account validation information, Emirates NBD aims to enhance cross-border payments security for participants on the Kinexys Liink network.

Anith Daniel, Group Head of Transaction Banking Services, Emirates NBD, said, "We are pleased to integrate with 'Confirm' by Kinexys Liink, which positions us at the forefront of payment innovation. By leveraging a blockchain network infrastructure such as the one from Kinexys by J.P. Morgan, we are able to provide real value to banks on the network, ensuring advanced payment security and streamlined operations. As the Kinexys Liink network expands, we

are excited about the future opportunities this collaboration will unlock."

Through the collaboration, Emirates NBD aims to provide participating banks and financial institutions on the network with enhanced security and efficiency and offer benefits to further streamline cross-border payment flows in the United Arab Emirates (UAE). Leveraging the 'Confirm' Application, Emirates NBD, will be able to validate account information for accounts based in the UAE for participants on the 'Confirm' Application.

Kinexys Liink is offered by Kinexys by J.P. Morgan – the firm's blockchain business unit focused on groundbreaking innovation to build the next-generation of financial infrastructure utilising blockchain technology. An Application on the Kinexys Liink network, 'Confirm' enables the global validation of bank account information in advance of payment being made. By providing validation services on the 'Confirm' Application Emirates NBD will help network participants ensure that

payments are routed correctly, preventing costly delays and reducing the occurrence of payment returns due to incorrect or outdated details. This will also help to control operational costs, improve straight-through processing rates, and help reduce payment delays, which could otherwise take several days to resolve, ensuring payments will reach the intended recipients quickly and efficiently.

Naveen Mallela, Global Co-Head of Kinexys by J.P. Morgan, said: "We are pleased to welcome Emirates NBD as part of the Kinexys Liink network. We are committed to developing solutions that enhance the speed, security and reliability of global cross-border payments and Emirates NBD's integration with the Kinexys Liink network helps bring these benefits to the region."

The collaboration positions Emirates NBD as a regional pioneer in utilising blockchain technology to streamline international payments, strengthening its commitment to innovation and payment security.

HID REDEFINES PHYSICAL AND DIGITAL SECURITY INTEGRATION

HID, global leader in trusted identity

and access management solutions, recently announced the launch of HID Integration Service, a platform that integrates physical security, cybersecurity and digital identity management.

This integration platform-as-a-service (IPaaS) was designed to empower application developers, solution integrators and software vendors to seamlessly and rapidly integrate essential physical security solutions, streamlining processes and enhancing system interoperability. By doing so, the platform aims to ease the burden of maintenance and upgrades associated with managing and implementing integrations between physical security and cybersecurity systems, thereby lowering costs, streamlining operations and significantly reducing implementation time.

“Organisations have long struggled with brittle, complex integrations and the costs to maintain them”, said Martin Ladstaetter, Senior Vice President and Head of Identity and Access Management Solutions at HID. “HID Integration Service eliminates these pain points by providing an integration platform that connects physical and digital security products, reducing time to market for development partners who are building

the next generation of security solutions with greater speed, quality, resilience and value.”

HID Integration Service directly addresses the top benefits security leaders seek from unified management solutions—improved efficiencies, simplified management and enhanced visibility—helping them:

- Reduce operational complexities and maintenance costs.
- Deliver new security capabilities faster into tailored industry solutions.
- Simplify security touchpoints through streamlined user experiences.

Key features include:

- A comprehensive integration layer that scales from point-to-point connections into multi-party integrations
- Pre-built integrations that accelerate deployment and reduce development costs
- Scalability and security to support rapidly evolving business needs

HID is privileged to have a few early adopters on the platform. Each brings deep expertise and robust capabilities across various technologies, verticals and security domains.

“We are excited about HID’s new

integration platform capabilities, which we believe can only add to SwiftConnect’s ability to meet our customers’ expectations and broader needs in the commercial real estate and enterprise markets”, according to Matt Kopel, co-founder and co-CEO of SwiftConnect. “The alignment of vision and direction between our companies will enhance and multiply the business changes our customers are pursuing”, continued Kopel.

“We envision a world where ID photos magically arrive in their intended location without human intervention”, said Luke Rettstatt, chief executive officer of CloudCard. “To realise this vision, we must develop and maintain many integrations, which is daunting for a small team. HID Integration Service allows us to focus on RemotePhoto’s AI workflow rather than building and maintaining certified integrations with third parties”.

This growing demand for seamless integration and efficiency is reflected in HID’s 2025 State of Security and Identity Report. According to the report, 67% of security leaders are actively transitioning to software-driven security solutions, with nearly three-quarters of organisations considering unified data collection critical to their operations.

MORE THAN 1 BILLION AI AGENTS SPAWN A VAST NEW CYBER ATTACK SURFACE: SANDBOXAQ LAUNCHES NEW PLATFORM TO ADDRESS THE THREAT

SandboxAQ, a leader in AI and

cybersecurity solutions, has announced the general availability of AQtive Guard, a groundbreaking platform designed to manage and secure Non-Human Identities (NHIs) and other cryptographic assets used by AI agents – both friendly and malevolent – that are surging across enterprise environments.

As billions of AI agents flood enterprise ecosystems, organizations

are facing an unprecedented surge of intelligent, adaptive cyber threats capable of continuously probing networks, evading detection, and rapidly exploiting vulnerabilities. This escalating threat demands proactive, AI-driven cryptographic defenses to counteract attacks that evolve faster than traditional security measures can respond.

AQtive Guard’s Discover module enables organizations to maintain an

accurate inventory and control over both NHIs and cryptographic assets such as keys, certificates, algorithms, and libraries, and is crucial for compliance and meeting regulatory mandates. AQtive Guard’s Protect orchestrates automated remediation workflows and enforces protection policies such as credential rotation or certificate renewal.

Leveraging its industry-leading Large Quantitative Models (LQMs), AQtive

Guard's Discover and Protect modules provide organizations with unprecedented visibility, control and remediation, addressing the escalating challenges of machine-to-machine communication security, compliance pressures, and the transition to the new NIST security standards.

As part of the launch, SandboxAQ also announced two key capabilities:

- Robust integration with the CrowdStrike Falcon® cybersecurity platform, representing SandboxAQ's deepest technical integration to date. AQtive Guard empowers joint customers with full visibility into their non-human identity and cryptographic inventories and vulnerabilities by pulling data directly from CrowdStrike endpoints. One-click ingestion translates to value from the first hour of use. AQtive Guard can then remediate the vulnerabilities as they are identified.
- Interoperability with Palo Alto Networks, a trusted name in enterprise security solutions. SandboxAQ is ingesting Palo Alto Networks' firewall logs directly into AQtive Guard, resulting in key visibility improvements for network security posture, vulnerability detection, and security compliance.

"There will be more than one billion AI agents with significant autonomous power in the next few years," stated Jack Hidary, CEO of SandboxAQ. "Enterprises are giving AI agents a vastly increased range of capabilities to impact customers and real-world assets. This creates a dangerous attack surface for adversaries. AQtive Guard's Discover and Protect modules address this urgent issue."

"As organizations accelerate AI adoption and the use of agents and machine-to-machine communication across all business domains and functions, maintaining a real-time, accurate inventory of NHIs and cryptographic assets is an essential cybersecurity practice. Being able to automatically remediate vulnerabilities



Marc Manzano, General Manager of Cybersecurity at SandboxAQ.

and policy violations identified is crucial to decrease time to mitigation and prevent potential breaches within the first day of use of our software," said Marc Manzano, General Manager of Cybersecurity at SandboxAQ.

AQtive Guard addresses these challenges by providing a unified, AI-driven solution for modern NHI and cryptography management. The platform offers:

- **Vulnerability Detection and Inventory:** Builds a complete and continuously updated inventory by integrating data from multiple sources, including existing data and meta-information captured from existing cybersecurity platforms and configuration management database tools. AQtive Guard works across the leading cloud providers including Amazon Web Services (AWS) and Google Cloud (GCP). This unified global inventory forms the crucial foundation for LQM analysis.
- **AI-powered Insights, Prioritization and Risk Analysis:** Applies SandboxAQ's industry-leading Cyber LQM to the unified inventory. By leveraging meta-data for advanced filtering and clustering, the platform enables efficient, noiseless exploration and accurate root-cause analysis, and delivers prioritized, actionable



Jack Hidary, CEO of SandboxAQ.

insights with contextual guidance for remediation and risk reduction, effectively reducing false positives. An integrated GenAI assistant further supports teams in understanding how to navigate relevant standards and regulatory frameworks.

- **Automated Remediation and Lifecycle Management:** Streamlines and automates the entire lifecycle of identities and cryptographic keys – including issuance, rotation, and revocation – reducing manual overhead and minimizing the risk associated with stale or compromised secrets.
- **Compliance and NIST Standards:** Provides targeted remediation recommendations, a powerful query engine with pre-built rulesets for major compliance standards (and custom query capabilities), and robust reporting to demonstrate compliance and significantly accelerate migration to new NIST standards.

Priority access starts

AQtive Guard launches as a fully managed, cloud-delivered platform built for rapid deployment and immediate impact in securing cryptographic assets and nonhuman identities. Organizations can secure priority access today for early deployment and risk assessments.

SENTINELONE RECOGNIZED AS 'BEST PERFORMING VENDOR' IN FROST RADAR ENDPOINT SECURITY, 2025

Company's AI-powered endpoint security earns best-in-class status with top marks for performance, growth, and innovation

SentinelOne, a global leader in

AI-powered security, has been named the best performing vendor on the Frost Radar: Endpoint Security, 2025, and a leader on both the Growth and Innovation indexes for its Singularity Endpoint Security Solution ahead of all other vendors evaluated.

"Leveraging cutting-edge AI technology in SentinelOne's Singularity Platform, SentinelOne empowers SecOps teams to stay ahead of sophisticated threats through automated workflows and rapid, real-time responses, with extensive technology integrations delivering comprehensive protection and operational efficiency," said Ozgun Pelit, Sr. Industry Analyst, Frost and Sullivan. "This combination of automation and human expertise strengthens defense capabilities, reduces response times and fosters trust-based relationships with customers by delivering consistent, effective outcomes."

Frost & Sullivan independently analyzed and ranked 13 industry leaders based on their solutions' effectiveness across 5 key capabilities on both the Innovation and Growth axis' and placed SentinelOne as the top-performing vendor overall. The company was also recognized for its strengths in the following areas:

- **Autonomous Innovation:** SentinelOne disrupted the endpoint market with AI-powered protection using static and behavioral AI to prevent advanced malware and automate ransomware remediation. Through the advent of generative AI solutions and continued innovation, the launch of Purple AI further strengthens SentinelOne's autonomous security capabilities, by bringing AI-enhanced triage, hunting, and investigation to the Singularity Platform. This past year, the Singularity Platform showcased industry-leading innovation in the MITRE ATT&CK 2024 Enterprise Evaluations, achieving



Braden Preston, Senior Director of Product Management, SentinelOne.

100% detection with zero delays across all steps and operating systems. By detecting all 16 attack steps and 80 substeps, SentinelOne demonstrated its ability to defend against sophisticated real-world threats.

- **Scalability:** SentinelOne leads Frost and Sullivan's Growth Index, driven by technology differentiation, strategic partnerships, and an expanding market footprint. Beyond endpoint security, SentinelOne has broadened its reach into Identity, Cloud, and AI SIEM, fueling rapid growth. Additionally, SentinelOne's platform integrates seamlessly with third-party security solutions, simplifying user onboarding and threat visibility. By leveraging a robust partner ecosystem and AI-powered security, SentinelOne continues to scale its business while delivering enhanced protection across the modern attack surface.

- **Growing Ecosystem:** SentinelOne delivers Singularity Endpoint through a global ecosystem of more than 5,000 partners, in addition to tens of thousands indirectly supported through our Managed Service Distribution and Marketplace partners that cast a wide net over the cybersecurity market.

"Being named the top-performing vendor and leader in Growth and Innovation in Frost and Sullivan Radar 2025 is a testament to SentinelOne's commitment to defining the future of AI-powered cybersecurity," said Braden Preston, Senior Director of Product Management, SentinelOne. "This recognition reinforces our position as the leader in endpoint security and highlights our ability to deliver autonomous, scalable protection that empowers organizations to outpace adversaries, unify their defenses and stay ahead of evolving threats."

Secure Your **Digital Future**

Simple. Secure. Resilient.



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

www.raqmiyat.com
UAE | KSA | INDIA



FORGING THE FUTURE OF CYBERSECURITY TALENT IN MIDDLE EAST AND AFRICA

I UNDER THE LEADERSHIP OF NED BALTAGI, SANS INSTITUTE IS BRIDGING EDUCATION, INDUSTRY, AND INNOVATION TO BUILD A SKILLED, SELF-RELIANT CYBERSECURITY WORKFORCE ACROSS THE REGION.

Cyber resilience is emerging as a national imperative in the Middle East and Africa, where digital transformation is accelerating across sectors. In this evolving landscape, the ability to anticipate, withstand, and recover from cyber threats depends not only on technology but also on a skilled local workforce. SANS Institute is taking a leading role in addressing this need through its practical training programs, strategic partnerships, and alignment with national cybersecurity frameworks.

By nurturing in-region talent, running Cyber Academies, and supporting capacity-building projects, SANS is helping shape a self-sustaining cybersecurity ecosystem across the region under the leadership of Ned Baltagi, Managing Director, Middle East, Africa, and Turkey.

Baltagi is a seasoned cybersecurity executive with over two decades of experience spanning IT, information security, and business leadership. He leads efforts to strengthen the region's

cybersecurity workforce through strategic programs, partnerships, and skills development initiatives.

Baltagi's career began in the early '90s with a milestone achievement – becoming one of the first 100 professionals globally to complete the Microsoft Certified Solutions Expert (MCSE) exams. He went on to work with Fortune 100 and 500 companies including Sprint Paranet, Compaq (later HP), Halliburton, and KBR, where he led digital transformation projects and quickly rose through the ranks due to his systems expertise and problem-solving ability.

He later channelled his entrepreneurial drive into founding startups across fintech, machine learning, and AI. With a global footprint spanning the US, Middle East, and Africa, Baltagi brings deep cross-sector insight to his role, delivering end-to-end cybersecurity solutions to enterprises and governments, and supporting national initiatives across Saudi Arabia, the UAE, Qatar, Bahrain, and beyond.

In an interview with Sandhya D'Mello,

Technology Editor at CPI Media Group, Baltagi — a degree holder in Computer Information Technology and IT Project Management — outlines the challenges, frameworks, and collaborative efforts shaping the future of cybersecurity resilience. He remains passionate about building sustainable cybersecurity talent pipelines throughout the region.

How would you define national cyber resilience in the context of the Middle East and Africa, and why is local capacity building crucial to achieving it?

National cyber resilience can be summarized as a nation's ability to anticipate, withstand, and rapidly recover from cyber threats while maintaining critical services and infrastructure. In a region undergoing rapid digital transformation such as the Middle East and Africa, true cyber resilience isn't just about having advanced technologies, but it depends heavily on cultivating skilled local talent that can adapt to evolving threats.

Local capacity building is imperative to this effort, and bridging the gap between

education and industry is a key first step. Universities must align their programs with real-world cybersecurity demands by collaborating with technology leaders and embedding hands-on training into their curricula. At the same time, organizations must invest in structured internships and mentorships to prepare students for actual challenges on the ground. These efforts strengthen the workforce and create a self-sustaining talent pipeline within the region.

Moreover, continuous training and development for existing professionals is necessary too. The threat landscape is shifting as we speak, and only a workforce that's regularly upskilled through certifications, practical simulations like Cyber Ranges, and leadership development, can respond effectively. Empowering local professionals with both technical and leadership capabilities ensures that cybersecurity decisions remain rooted in regional context and are less dependent on external expertise.

With both governments and private sectors investing heavily in internal cybersecurity teams, how is SANS supporting this shift across the region?

A region's cybersecurity readiness should be strengthened from the inside out. At SANS, we go beyond traditional training models and focus on the practical development of high-performing internal security teams. We work closely with cybersecurity managers and HR leaders across the Middle East to understand what makes security teams truly effective, and how to build them sustainably. Through in-depth research, such as the SANS 2025 | GIAC Workforce Study, we can



provide organizations with actionable insights rooted in real-world data. This includes case studies and survey results that highlight what's working across the region, allowing talent managers to make informed decisions for their specific organizational needs.

Companies need to embrace skills-based hiring, adopt workforce

frameworks, and prioritize skills development over simply expanding headcount. We emphasize the importance of developing internal talent pathways, refining job requirements to better match real-world roles, and diversifying the talent pool through expanded recruitment channels. Our hands-on training and certification programs empower teams to tackle current and future cybersecurity challenges with confidence. We also encourage organizations to secure executive sponsorship, ensuring cybersecurity remains a strategic priority at the highest levels.

“HANDS-ON TRAINING ALSO HELPS PROFESSIONALS RETAIN KNOWLEDGE MORE EFFECTIVELY, BRIDGING THE GAP BETWEEN THEORY AND REAL-WORLD APPLICATION”

What are the most significant challenges faced by the current cybersecurity workforce in the Middle East?

The cybersecurity workforce challenge in the Middle East goes beyond simply hiring more professionals. It's about finding, developing, and retaining individuals with the right mix of technical expertise and adaptability. One major hurdle is aligning workforce expectations with modern workplace norms. Today's cybersecurity professionals value flexibility and autonomy, making it essential for organizations to offer remote or hybrid work models and shift performance evaluations toward outcome-based metrics.

Another significant challenge lies in the structural approach to cybersecurity. Traditional centralized models are no

longer sufficient. Organizations must decentralize cybersecurity practices by embedding security responsibilities across various technical roles like DevOps and network engineering. This "federated" approach promotes shared accountability and ensures security is considered at every stage of operations and development.

"THE THREAT LANDSCAPE IS SHIFTING AS WE SPEAK, AND ONLY A WORKFORCE THAT'S REGULARLY UPSKILLED THROUGH CERTIFICATIONS, PRACTICAL SIMULATIONS LIKE CYBER RANGES, AND LEADERSHIP DEVELOPMENT CAN RESPOND EFFECTIVELY"

Recruitment also presents a challenge, often due to a disconnect between HR and technical teams. Effective hiring requires collaboration; HR must have a basic understanding of cybersecurity roles, while technical leads should help assess candidate suitability. Without this alignment, organizations risk missing out on capable talent.

Finally, diversity remains a pressing concern. Gender representation in cybersecurity is still lacking, and organizations need to take deliberate steps to build inclusive environments. This includes partnering with educational institutions, supporting STEM initiatives, and launching mentorship programs for underrepresented groups.

From your perspective, what are the biggest skill gaps in regional cybersecurity teams today?

A core challenge facing the industry is building and retaining professionals who have the right mix of skills and capabilities. Across the region, a major skill gap exists in hands-on technical expertise, particularly in areas like cloud security, incident response, threat hunting, and secure software development. Many teams also lack professionals with the ability to translate complex technical risks into business-relevant insights, an increasingly vital skill for influencing leadership decisions. Additionally, there is often limited internal mobility due to a lack of clear talent development pathways, leading to stagnant growth and high attrition. Soft skills, such as communication and collaboration, are also in short supply,



yet they are critical in cross-functional security environments. Closing these gaps requires not only targeted training and certification but also a cultural shift toward continuous learning, mentorship, and strategic workforce planning across both public and private sectors.

How does the SANS curriculum align with national cybersecurity frameworks such as Saudi Arabia's SCyWF and the NCA's strategy?

The Saudi Cybersecurity Workforce Framework (SCyWF) serves as a comprehensive guide for standardizing cybersecurity work roles across various industries in Saudi Arabia. By aligning these roles with those in other sectors, the SCyWF establishes a clear structure that ensures consistency in an ever-evolving field. The framework categorizes cybersecurity work, defines specific roles, and sets requirements based on TKSA – tasks, knowledge, skills, and abilities.

Designed to foster collaboration between sectors such as utilities/tech or healthcare/retail, the SCyWF helps organizations define job requirements for both security teams and HR departments. Developed by the National Cybersecurity Authority (NCA), the authority responsible for overseeing cybersecurity in the Kingdom, the SCyWF supports the NCA's mission to protect Saudi Arabia's vital interests, national security, critical infrastructure, priority sectors, and government services.

To help support workforce development, SANS has mapped our courses and certifications to the SCyWF work roles. This enables organizations to easily identify training options that align with the skills needed for each specific role. With over 70 courses developed by leading cybersecurity experts, SANS provides real-world training, including lab-based testing and scenarios, to ensure your team is equipped with practical skills and validated through certification to meet the demands of the rapidly evolving cybersecurity landscape.



“BUILDING A MEANINGFUL CAREER IN CYBERSECURITY IS AS MUCH ABOUT TECHNICAL EXPERTISE AS IT IS ABOUT SHOWING INITIATIVE AND STAYING INVOLVED. THE MORE YOU GIVE TO THE COMMUNITY, THE MORE IT GIVES BACK”

What role does SANS play in helping national stakeholders localize training and build sustainable cybersecurity talent pipelines?

We offer tailored programs that align with regional needs and workforce development goals. Through initiatives like our Cyber Academies, we collaborate with governments and national entities to equip local talent with practical, industry-relevant skills. These programs are designed to be inclusive, accessible, and results-driven, often leading to globally recognized GIAC certifications that open doors to long-term careers in cybersecurity. We also support sustainability by reinforcing continuous learning into the training journey – from mentorship to skills assessments and advanced pathways that allow professionals to grow into leadership roles and build their own teams.

Can you highlight a specific partnership or project where SANS has contributed to national cybersecurity capacity building in the region?

Our Cyber Academy initiative in Bahrain, in collaboration with a government entity – where we delivered an intensive eight-week training program for Bahraini nationals aged 18 and above, culminating in three GIAC certifications. This initiative directly addressed the local cybersecurity skills gap and empowered participants with globally recognized credentials to launch or advance their careers. Similarly, we ran two Cyber Academies in Kuwait, designed to equip participants with practical skills to combat evolving threats in high-stakes sectors. These academies are part of our broader commitment to delivering targeted, results-driven training that supports both individuals and national cybersecurity objectives.

What impact have hands-on training programs and simulations had on improving workforce readiness and resilience across the region?

Traditional classroom learning alone

→ **“MANY TEAMS ALSO LACK PROFESSIONALS WITH THE ABILITY TO TRANSLATE COMPLEX TECHNICAL RISKS INTO BUSINESS-RELEVANT INSIGHTS, AN INCREASINGLY VITAL SKILL FOR INFLUENCING LEADERSHIP DECISIONS”**

can't prepare cybersecurity professionals for the dynamic nature of real-world threats. Hands-on training also helps professionals retain knowledge more effectively, bridging the gap between theory and real-world application. By practicing in high-pressure, simulated environments, teams are better prepared to act decisively during actual incidents, making this type of training essential for long-term operational readiness. Interactive, instructor-designed environments replicate real-world networks, systems, and applications in a safe, controlled setting. Whether it's identifying vulnerabilities, responding to simulated attacks, or defending critical infrastructure, individuals and teams gain valuable, practical experience without the risk of impacting live environments. Moreover, the ability to customize these simulations means that organizations can align training with their specific security challenges and maturity levels.

How do you see the role of public-private collaboration evolving in the region's cybersecurity ecosystem?

As threats grow more complex and cross-sectoral, no single entity – government or private – can address them in isolation. We're seeing an encouraging shift toward shared responsibility, where national agencies, critical infrastructure providers, and private sector organizations are working in tandem to shape cybersecurity strategies, share threat intelligence, and align on workforce development priorities.

SANS actively supports this evolution by facilitating programs that bring both sides to the table. Our partnerships often involve government bodies and private companies co-sponsoring Cyber Academies,

contributing to curriculum development, or participating in region-specific research. These collaborations are key to building a unified, agile cybersecurity workforce equipped to protect both national and economic interests. As this model matures, we expect to see more integrated frameworks, shared training standards, and cross-sector simulations that drive collective resilience across the Middle East and Africa.

What advice would you offer to aspiring cybersecurity professionals in the region who are looking to build meaningful careers in the sector?

Be curious, committed, and connected. Cybersecurity is changing by the second, so keep adapting to modern learning frameworks and continuously upskill – whether through certifications, hands-on labs, or real-world simulations. Just as importantly, engage with your local cybersecurity community. Participate in forums, attend as many events as possible, and take advantage of community-driven opportunities.

At GISEC 2025, we're hosting the SANS GISEC Academy for the very same reason. That's three days of exclusive, free-to-attend sessions led by our expert instructors designed to help aspiring professionals gain valuable insights and practical knowledge. Participants will also receive a Certificate of Attendance once they complete the session, a small but important step in showcasing your commitment to the field. Building a meaningful career in cybersecurity is as much about technical expertise as it is about showing initiative and staying involved. The more you give to the community, the more it gives back. 🦋

Dr Ahmed Hamdan Al Zeyoudi,
Director of the Office of His Highness
the Crown Prince of Fujairah.

FUJAIRAH IGNITES TECH FUTURE WITH YOUNG TECHPRENEURS INITIATIVE

EMPOWERING 244 STUDENTS WITH AI, CODING, AND
CYBERSECURITY SKILLS THROUGH IMMERSIVE LEARNING
AND VISIONARY LEADERSHIP

Fujairah's Young Techpreneurs initiative launched its first edition in April 2025, organised by the Office of His Highness the

Crown Prince of Fujairah in collaboration with Hamdan bin Mohammed Smart University (HBMSU).

This initiative follows the directives of His Highness Sheikh Mohammed bin Hamad Al Sharqi, Crown Prince of Fujairah, and exemplifies how visionary leadership can shape the future by equipping youth with knowledge and transforming them from learners into founders.

The initiative, which aligns with the Crown Prince's vision to elevate the role of youth in the digital age, spans three months and includes 244 students—130 boys and 114 girls—from across Fujairah. Its core mission is to equip young participants with foundational and advanced skills in cybersecurity, programming, and artificial intelligence through a hands-on, project-based curriculum.

Participants benefit from interactive workshops, simulations, and global tech partnerships, gaining exposure to real-world applications of technology.

Upon successful completion, students will receive a certification accredited by HBMSU, the UAE's first accredited smart university.

In this exclusive interview, Dr Ahmed Hamdan Al Zeyoudi, Director of the Office of His Highness the Crown Prince of Fujairah, shares with Sandhya D'Mello, Technology Editor, CPI Media Group, long-term vision behind Fujairah's landmark initiative.

What inspired the launch of the Young Techpreneurs initiative?

The inspiration for the Fujairah's Young Techpreneurs initiative came directly from the visionary leadership of H.H. Sheikh Mohammed bin Hamad Al Sharqi, the Crown Prince of Fujairah to design a transformative programme that empowers a new generation of tech-savvy youth in Fujairah.

Further, following the directives of H.H. Sheikh Mohammed, Dr Mansoor Al Awar, Chancellor of Hamdan Bin Mohammed Smart University (HBMSU), who recognised its significance mobilised a dedicated team at HBMSU, in collaboration with CODE HUB, the strategic partner for youth skill development, to craft a comprehensive

framework that would position Fujairah as a national and regional leader in youth empowerment. The outcome was Fujairah's Young Techpreneurs initiative, a bold, multi-phased vision targeting students aged 7 to 15 with a unique and future-focused approach to techpreneurship.

Quoting the words of Radwa Salem, who is responsible for the academic and educational aspects of Fujairah's Young Techpreneurs initiative, it is a testament to what visionary leadership, strategic partnerships, and a shared commitment to the future can achieve. Moreover, the initiative aims to teach students how to use technology and help them discover how to shape the future with it.

With 244 students participating, how were the candidates selected, and what criteria were used to ensure a balanced representation of skills and interests across fields like cybersecurity, programming, and AI?

In alignment with the vision of H.H. Sheikh Mohammed, the initiative was made exclusively available to national students in Fujairah. Parents were invited to register their children through a dedicated HBMSU platform once the



initiative was publicly announced.

To elaborate on the selection process, a coordination team engaged with every registrant to ensure commitment, communicate expectations, and prepare students for participation. Rather than pre-screening based on prior experience, the initiative adopted an inclusive and developmental approach, dividing students into age-based cohorts and tailoring the curriculum accordingly to ensure all participants, regardless of their prior knowledge, could meaningfully engage and grow.

Could you elaborate on the hands-on educational model being used in the initiative? What makes this approach particularly effective for teaching complex tech topics to young students?

We believe students learn best by doing: through building, prototyping, collaborating, and solving real-world problems. Thus, the initiative follows a hands-on, experiential learning model.

We have integrated the world's most trusted educational platforms in AI, coding, and creative technologies, while partnering with global technology organisations to bring expertise across fields such as machine learning and cybersecurity. These partnerships ensure that students learn using tools and technologies shaping the global digital landscape. Whether developing AI models, designing games, or creating digital awareness campaigns, our classroom sessions are designed to be engaging and interactive, encouraging students to explore, experiment and create.



What role does Hamdan Bin Mohammed Smart University (HBMSU) play in the initiative, and how are their academic frameworks and faculty contributing to its success?

HBMSU serves as the academic foundation and institutional lead for the initiative. The university developed the entire educational vision and

curriculum, leveraging its expertise in smart learning and its long-standing commitment to innovation in education.

To elaborate on its contributions, HBMSU provided the smart digital platform for registration and communication; established certification frameworks that validate learning outcomes; led the training and overseeing of educational teams to ensure high-quality delivery and most significantly, the university granted students access to HBMSU's Cloud Campus, giving them the same digital learning experience and tools available to university-level learners. This integration offers the youth of Fujairah a head start in higher education and emerging technologies.

WE AIM TO STRENGTHEN FUJAIRAH'S POSITION AS A NATIONAL AND REGIONAL LEADER IN YOUTH EMPOWERMENT AND DIGITAL INNOVATION, CREATING A MODEL THAT WILL INSPIRE OTHER COMMUNITIES AND BE SHARED AS A BEST PRACTICE ACROSS THE UAE AND BEYOND.




THE INSPIRATION FOR THE FUJAIRAH'S YOUNG TECHPRENEURS INITIATIVE CAME DIRECTLY FROM THE VISIONARY LEADERSHIP OF H.H. SHEIKH MOHAMMED BIN HAMAD AL SHARQI, THE CROWN PRINCE OF FUJAIRAH TO DESIGN A TRANSFORMATIVE PROGRAMME THAT EMPOWERS A NEW GENERATION OF TECH-SAVVY YOUTH IN FUJAIRAH.

Looking ahead, what are the expected outcomes or long-term goals of the Young Techpreneurs initiative for both the participants and the wider Fujairah community?

Through this forward-thinking program, we aim to strengthen Fujairah's position as a national and regional leader in youth

empowerment and digital innovation, creating a model that will inspire other communities and be shared as a best practice across the UAE and beyond.

There are two key long-term goals for the initiative, which currently is in its first edition:

- **Fujairah's First Youth Innovation Incubator:** The initiative will culminate in the launch of a dedicated Youth Techpreneur Incubator, the first of its kind in Fujairah. This incubator will provide young talents with the support and resources they require to develop real-world solutions. Furthermore, it will empower students to transform their ideas into implementation, creating social and economic value across the community.
- **Sustainable Talent Development:** With new cohorts joining each phase, the initiative aims to ensure a continuous stream of future tech leaders and entrepreneurs. This model guarantees that the Fujairah Youth Techpreneur Incubator will remain an active, evolving space for innovation for years to come. 

SECURITY IS EVERYONE'S RESPONSIBILITY, SAYS GENETEC'S FIRAS JADALLA

Genetec Inc., a global technology company transforming the physical security industry for over 25 years, recently held empower360 roadshow in Dubai, bringing together industry professionals to explore the future of physical security.

The event highlighted key advancements in video analytics, access control, and the growing shift toward hybrid security deployments. It emphasized the importance of open architecture, IoT integration, and unified security solutions, offering guidance on best practices for upgrading legacy systems while preserving existing investments.

Attendees participated in interactive sessions, networked with peers, and gained insights from Genetec experts on how physical security is becoming more resilient, data-driven, and essential to enhancing urban safety. The roadshow equipped security professionals with practical knowledge to support the UAE's evolving focus on building smarter and safer cities.

Firas Jadalla, Regional Director for the Middle East, Turkey & Africa at Genetec spoke to Daniel Shepherd from CPI Media Group at the Genetec empower360 roadshow in Dubai. The event delved into the importance of open architecture and IoT technologies in developing smarter cities. There was also a strong focus on new trends in

access control technology, simplifying video management and providing advanced scalable solutions.

With almost 20 years at the Genetec, Firas Jadalla has witnessed their humble beginnings in 2005, to its expansion across nine Middle Eastern cities. In addition to their focus in Dubai and Riyadh, Genetec has local teams in Doha, Cairo and Cape Town South Africa. They have also been recognised as a leader in innovation worldwide with headquarters in Montréal and offices in multiple countries.

Which security trends do you believe organisations should keep in mind when it comes to secure solutions?

When you consider security, we are seeing more awareness around cybersecurity which was triggered by the pandemic. We see more end users and system integrators looking for solutions that can meet the current challenges of cybersecurity. Another element is an increased focus on unification. 20 years ago, people were interested in the idea of having an interface between physical security solutions. They wanted to have

alarms, control systems and video feeds interfaced together, which we now know as integration. Today, the trends are more focused around unification. In integration multiple different systems are combined definitively for efficiency and unification represents a unique concept.

To elaborate on the last point, how does unified security differ from current security solutions businesses use?

When we talk about a built-in unified product there is a big difference between that and an integrated solution. A unified solution is built from the ground-up with the same code and aspects as most physical products. With unified solutions we take one solution that can meet all your requirements such as physical security, video management, access control system, license distribution system, intercom and more. Some projects might not require all these features, but broadly it provides one solution with one interface. Consider it like Microsoft Office which includes Excel, PowerPoint and Word under a familiar interface. With the Genetec Unified Platform, it is one platform

HYBRID OFFERS THE BEST OF BOTH WORLDS AS YOU CAN ADDRESS ISSUES RELATED TO BANDWIDTH AND THE COST OF BANDWIDTH WHILST BEING ABLE TO USE CLOUD ACCESS FROM ANYWHERE TO GATHER INSIGHTS.



Firas Jadalla, Regional Director for the Middle East, Turkey & Africa at Genetec.



and one interface that meets all these requirements in a seamless package. This is advantageous because it becomes easier to deploy, train employees or perform updates without breaking any links.

Do you see cloud security solutions becoming more common or is hybrid still popular with your customers?

All of us in Genetec agree that the cloud is going to dominate the future of security solutions. For us it is not a question of will, it is a question of when. When will we see this adoption reach over 50%? When will over 50% of physical security installations rely on an on-prem cloud? When you look at enterprise solutions, there is a bigger appetite for hybrid verses cloud. If we look at small deployments like shop cameras, the owners will likely prefer everything to be linked via cloud. However, with bigger examples like airports that use

thousands of cameras it becomes more meaningful and cost effective to use a hybrid solution. Hybrid offers the best of both worlds as you can address issues related to bandwidth and the cost of bandwidth whilst being able to use cloud access from anywhere to gather insights.

Can your security centre solutions incorporate and develop alongside the changes we are seeing in access control technology?

Our flagship product offers a unified platform for management control. What you get with this platform is that every time a software update is available you only need to do it once to keep things running smoothly. There are no unnecessary integration links or interfaces. Our latest products feature an element called GUS (Genetec Upgrade Service) which when enabled, automatically checks for updates during night hours.

Before we wrap up, is there anything else you would like to say to our readers?

Genetec has taken a very strong stance on cybersecurity since 2016. We've seen people become aware of the importance of having a secure security solution right after the pandemic. During that time more people were working from home leading to an increase in the number of cyberattacks. We've continued to encourage our system integrator, channel partners and end users to give cybersecurity the importance it is due. At Genetec, we have improved our solutions with built-in cybersecurity and created guidelines for our system integrator during deployment to tighten security measures. Our solution includes many features such as, encryption to avoid man-in-the-middle attacks between cameras and the servers' workstation. I would like to take this opportunity to remind people of the critical nature of their own security systems and at the end of the day it is everyone's responsibility. Whether it's Genetec being the supplier, our system integrator deploying it or the end user running it, everyone is accountable. We must all work together to share the responsibility. 🛡️

GENETEC HAS TAKEN A VERY STRONG STANCE ON CYBERSECURITY SINCE 2016. WE'VE SEEN PEOPLE BECOME AWARE OF THE IMPORTANCE OF HAVING A SECURE SECURITY SOLUTION RIGHT AFTER THE PANDEMIC.



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



WORLD PASSWORD DAY: REPLACING THE WEAKEST LINK WITH SMARTER SECURITY

EXPERTS URGE ENTERPRISES TO DITCH OUTDATED PASSWORD ROUTINES FOR BEHAVIOR-DRIVEN, PASSWORDLESS SOLUTIONS AS CYBER THREATS EVOLVE.



World Password Day is no longer just a day to reset a password—it's a wake-up call.

As cyberattacks become more sophisticated, industry leaders agree: the password, once the gatekeeper of digital identity, has become the weakest link. From evolving best practices to the behavioral science behind poor password hygiene, experts across the cybersecurity spectrum are calling for a fundamental shift in how organizations approach authentication.

World Password Day, observed on the first Thursday of May, was established in 2013 by Intel Security to raise awareness about the importance of strong password practices. Inspired by security expert Mark Burnett's call to dedicate a day to password hygiene, the day



Chester Wisniewski, Director, Global Field CISO at Sophos

encourages individuals and organizations to strengthen their digital defenses through secure passwords, multi-factor authentication, and passwordless technologies.

The first line of defense: strengthen it or replace it

"A strong password is your first barrier; don't let it be the weakest link," says Ezzeldin Hussein, Regional Senior Director, Solution Engineering – META at SentinelOne. "A password is more than just a key; it's the gateway to your digital identity. Strengthen it, protect it, and complement it with multi-factor authentication. On World Password Day, let's commit to better security habits—because a strong password today means a safer digital world tomorrow."

Passwords remain foundational to digital security—but they must evolve. Hussein advocates for strong, unique passwords backed by multi-factor authentication (MFA) and password managers. More importantly, he emphasizes a shared responsibility: users and organizations must adopt secure habits and champion next-generation alternatives like biometrics and passkeys.

The end of the password: a necessary evolution

"We need to move away from reliance on passwords and shared secrets,"



Ezzeldin Hussein, Regional Senior Director, Solution Engineering – META, SentinelOne

ACCESS KEYS OR PASSKEYS TODAY REPRESENT THE MOST ROBUST SOLUTION FOR BUILDING A FUTURE WITHOUT PASSWORDS, PHISHING, AND, HOPEFULLY, LARGE-SCALE COMPROMISE.

CHESTER WISNIEWSKI, DIRECTOR AND GLOBAL FIELD CTO AT SOPHOS.

insists Chester Wisniewski, Director and Global Field CTO at Sophos. “Access keys or passkeys today represent the most robust solution for building a future without passwords, phishing, and, hopefully, large-scale compromise.”

Sophos’ 2025 Active Adversary Report reveals that compromised credentials remain the top cause of cyber incidents for the second consecutive year. Traditional authentication methods—whether passwords or MFA codes—are being bypassed through advanced phishing kits and cookie theft.

Wisniewski endorses WebAuthn, a protocol that leverages cryptographic key pairs and physical devices, including biometrics. This model not only prevents phishing but also authenticates both the user and the service—making unauthorized access significantly harder.

Understanding why password fatigue persists

“It’s not that people don’t understand the risks. It’s that the need for uninterrupted access often outweighs the promise of long-term protection,” explains Nireesh Swamy, Enterprise Evangelist at ManageEngine.

Swamy examines the human side of cybersecurity—specifically the psychological patterns that drive password fatigue, reuse, and weak security habits. Concepts like bounded rationality, availability heuristics, and loss aversion reveal that the struggle with passwords isn’t about ignorance, but about mental efficiency.

Organizations often respond with stricter protocols, but Swamy argues that the real fix lies in removing the need for passwords altogether. Solutions such as passkeys, Single Sign-On (SSO), and

ON WORLD PASSWORD DAY, LET’S COMMIT TO BETTER SECURITY HABITS—BECAUSE A STRONG PASSWORD TODAY MEANS A SAFER DIGITAL WORLD TOMORROW.

EZZELDIN HUSSEIN, REGIONAL SENIOR DIRECTOR, SOLUTION ENGINEERING – META AT SENTINELONE.



Nireesh Swamy, Enterprise Evangelist at ManageEngine

magic links reduce cognitive load and eliminate the risk of human error

Designing behavior-aware systems

To effectively tackle risky password behavior, organizations must bridge the gap between convenience and security. That means:

- Adopting passkey-enabled vaults to eliminate password memorization.
- Using SSO to centralize access and reduce the number of logins.
- Deploying PAM (Privileged Access Management) solutions that automate, restrict, and audit access.
- Embedding AI into access control policies to detect and prevent

standing privileges and risky behavior in real-time.

These are not just security upgrades—they’re behavioral interventions. “When an organization removes decision points where things go wrong, they’re not just securing systems—they’re correcting flawed human design,” Swamy notes.

Policy must match progress

The technological path forward is clear, but without supportive policy, security tools lose their impact. Shared credentials, over-permissioning, and legacy access controls remain common pitfalls. Progressive companies are implementing dynamic, AI-powered access policies that adjust privileges based on context and usage—reducing friction while increasing protection.

Rethinking the absurdity of passwords

“In many ways, our daily interactions with passwords feel a lot like Sisyphus’ burden,” Swamy reflects. “We push the boulder uphill every day, only to start over. The solution is not to make the boulder lighter. It’s to remove the hill.”

Tools like passkeys, SSO, PAM, and AI do more than simplify access—they eliminate the absurdity of forcing humans to defend digital fortresses with mental gymnastics. When systems account for how people actually think and behave, security becomes sustainable.

This World Password Day, the message is unified and urgent: secure systems must evolve beyond passwords. Whether by strengthening existing routines with MFA and password managers or by advancing toward passwordless authentication, the time for action is now. Because as our digital lives expand, so too must the way we protect them. 🛡️

ACCESS KEYS OR PASSKEYS TODAY REPRESENT THE MOST ROBUST SOLUTION FOR BUILDING A FUTURE WITHOUT PASSWORDS, PHISHING, AND, HOPEFULLY, LARGE-SCALE COMPROMISE.

CHESTER WISNIEWSKI, DIRECTOR AND GLOBAL FIELD CTO AT SOPHOS.



معرض و مؤتمر الخليج العالمي لأمن المعلومات

GISEC

GLOBAL

06 - 08 MAY 2025

DUBAI WORLD TRADE CENTRE

HOSTED BY

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



OFFICIAL GOVERNMENT CYBERSECURITY
PARTNER

مركز الأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER



OFFICIALLY SUPPORTED BY



وزارة الداخلية
MINISTRY OF INTERIOR

شرطة دبي
DUBAI POLICE



MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT

SCAN HERE



GET INVOLVED

OFFICIAL DISTRIBUTION
PARTNER



LEAD STRATEGIC
PARTNER



STRATEGIC PARTNER



DIAMOND SPONSOR



PLATINUM SPONSOR



GOLD SPONSOR



GOLD SPONSOR



BRONZE SPONSOR



BRONZE SPONSOR



CTF PARTNER



CONTACT US

gisec@dwtc.com

+971 4 308 6469

cyber.gisec.ae

[#gisecglobal](https://twitter.com/gisecglobal)

HUAWEI TO SHOWCASE AI-POWERED CYBERSECURITY SOLUTIONS AS LEAD STRATEGIC PARTNER OF GISEC GLOBAL 2025

EVENT BRINGS TOGETHER OVER 25,000 CYBERSECURITY PROFESSIONALS FROM MORE THAN 160 COUNTRIES TO ADDRESS EVOLVING THREATS IN AN INCREASINGLY AI-DRIVEN LANDSCAPE.



Sean Yang, Global Cybersecurity and Privacy Protection Officer of Huawei.



uawei, a global leader in information and communications technology (ICT), will showcase

its comprehensive AI-powered cybersecurity solutions as the Lead Strategic Partner of GISEC Global 2025, Middle East and Africa's largest cybersecurity event. Taking place from May 6-8 at Dubai World Trade Center, the event brings together over 25,000 cybersecurity professionals from more than 160 countries to address evolving threats in an increasingly AI-driven landscape.

Thanks to the accelerating uptake of technologies such as 5G, cloud, and AI, our world is becoming digital, fully connected, and intelligent. Digital technologies have permeated every aspect of our lives, reshaping how we live and work through their openness and connectivity on a global scale. Cybersecurity has therefore become a top concern for many countries and industries worldwide. Building digital trust and ensuring cybersecurity, two cornerstones of guaranteeing digital transformation, have become a practice the international community is keen to pursue.

Sean Yang, Global Cybersecurity and Privacy Protection Officer of Huawei, said, "We are delighted to extend our long-term partnership with GISEC Global by becoming its Lead Strategic Partner for the 2025 edition. Huawei

is committed to securing our shared digital future with governments, industry organizations, standardization bodies, and enterprise stakeholders. Through such partnerships, we aim to be a reliable partner in the digital and intelligent world and provide our customers with competitive and secure product solutions."

At GISEC Global 2025, visitors to Huawei's booth can experience the company's latest cybersecurity innovations. These include comprehensive AI-native security solutions on Huawei Cloud, featuring Huawei Cloud's 1+7 Security Defense System and the AI-native cybersecurity center SecMaster; Xinghe Intelligent Network Security with unified SASE & EDR solutions utilizing a unique "cloud-network-edge-endpoint" architecture; Multilayer Ransomware Protection Solution that accurately detects ransomware, prevents horizontal proliferation, and ensures fast recovery; and All-Scenario Data Protection with 3-in-1 architecture design and industry-leading recovery performance.


Huawei will host several exclusive events during GISEC Global 2025. On May 6, the company will present an executive boardroom session where industry leaders will gather and dive into the latest advancements in AI-driven security, and Huawei Cloud security solutions. The same

day will feature a "Cyber Resilience Workshop", bringing together ICT network security experts to discuss evolving digital security challenges, covering lifecycle management, integrity protection, vulnerability management, and digital certificates.

On May 7, Huawei will conduct the "OceanClub Workshop: Data Protection in the AI Era", exploring AI-driven data security trends, advanced backup solutions, and ransomware defense with a live demonstration of Huawei's OceanProtect solutions. The "Xinghe Intelligent Network Security Forum" will also take place, discussing how enterprises can build SASE (Secure Access Service Edge) architecture to address challenges such as cloud service migration, local traffic outbound, and AI-generated threats.

The company will conclude its thought leadership program on May 8 with the "Cybersecurity Industry Practices Forum", bringing together regulators, industry leaders, experts, and scholars to explore cybersecurity opportunities and challenges, covering global legislation, supply chain security, AI security, and ransomware prevention.

Huawei's strategic presence at GISEC Global 2025 embodies the company's foundational belief that cybersecurity and privacy protection are the cornerstones of the digital and intelligent world. This philosophy drives the company's approach to developing security solutions where protection isn't merely added on but intrinsically built into every product from conception. Huawei champions a verification-based security model that relies on common standards, enabling objective assessment and fostering industry-wide trust through transparency and measurable security practices.

Huawei will exhibit at Hall 5, stand A180, at GISEC Global 2025. 

WE ARE DELIGHTED TO EXTEND OUR LONG-TERM PARTNERSHIP WITH GISEC GLOBAL BY BECOMING ITS LEAD STRATEGIC PARTNER FOR THE 2025 EDITION. HUAWEI IS COMMITTED TO SECURING OUR SHARED DIGITAL FUTURE WITH GOVERNMENTS, INDUSTRY ORGANIZATIONS, STANDARDIZATION BODIES, AND ENTERPRISE STAKEHOLDERS.



Sertan Selcuk, Vice President for METAP and CIS, OPSWAT.

OPSWAT ANNOUNCES GISEC 2025 PARTICIPATION WITH A FOCUS ON CRITICAL INFRASTRUCTURE

DEFENDING CRITICAL INFRASTRUCTURE WITH TRUSTED IT/OT CYBERSECURITY SOLUTIONS AT THE HEART OF GISEC GLOBAL 2025

OPSWAT, a global leader in Critical Infrastructure Protection (CIP) cybersecurity solutions, recently announced its participation as a Diamond Sponsor at MEA's leading security event, GISEC Global 2025.

The event will run from 6 to 8 May at the Dubai World Trade Centre, hosted by the UAE Cybersecurity Council in partnership with the Dubai Electronic Security Centre.

Industry professionals from around the world will be able to learn from thought leaders at OPSWAT, while the company aims to forge strategic alliances that drive mutual growth and success in addressing cybersecurity challenges.

"Our main focus at GISEC Global 2025 will be critical infrastructure, the lynchpin of economic progress and an increasingly popular target for threat actors", said Sertan Selcuk, Vice President for METAP and CIS, OPSWAT. "Our partnerships will involve devising ways of protecting the interconnected systems and technologies that drive the Fourth Industrial Revolution. Through our demonstrations and discussions at GISEC 2025, OPSWAT experts will show how our solutions directly address the latest cybersecurity challenges, especially the

ongoing merger of IT and OT".

CISO and industry visitors of GISEC can visit OPSWAT's CIP Mobile Lab, where OP/X Labs will provide live demos of industry-leading solutions that secure critical infrastructure, while OPSWAT experts offer practical insights into safeguarding organizations' most vital systems and networks.

Alongside the Mobile Lab will be OPSWAT's Nuclear Plant Model Reactor, a display that underscores the company's prowess in securing sensitive environments like nuclear power plants. Part of the demonstration will be the showcasing of the interconnectivity of the mobile lab with the nuclear plant model.

OPSWAT subject matter experts will also participate in speaking engagements and seminars at GISEC Global 2025. On day one, on the Dark Stage, OPSWAT will run a live hacking session to highlight the dangers that prowl today's threat landscape.


During day two, on the Government Stage, hosted by Dubai Electronic Security Center, OPSWAT Founder and CEO, Benny Czarny, will present "Breaking the Firewall: Revolutionizing Cyber Defence for a Connected World". He will make the case for a fundamental rethinking of the traditional firewall, highlighting how

the rise of AI-driven exploits, encrypted attacks, and increasingly complex network environments demands a new approach to cybersecurity.

Also on day two, on the Critical Infrastructure Stage, OPSWAT's Director of Products and Solutions, Kris Voorspoels, will take part in a panel discussion on the security crisis facing the Industrial Internet of Things (IIoT) in the regional oil and gas sector. With eyes on both 2025 and beyond, panel experts will discuss how the rise of IoT devices in the petrochemical industry, from pipeline sensors to drilling systems, has impacted security for one of the region's most important revenue streams.

Aiming to enhance cybersecurity standards across the region in alignment with the goals of the UAE National Cybersecurity Strategy, OPSWAT Academy will offer complimentary CIP certifications, such as File Security Associate (OFSA), Secure Storage Associate (OSSA), Email Security Associate (OESA), Web Traffic Protection Associate (OWPA), and Data Transfer Security Associate (ODSA).

"Our GISEC participation further demonstrates our steadfast commitment to delivering IT/OT cybersecurity solutions and fostering the cyber talent that the region needs to defend its critical infrastructure and sustain economic progress", Selcuk added. "MEA technology and business leaders increasingly look to OPSWAT to defend their IT/OT suites. We stand ready as their trusted partner".

At GISEC Global 2025, OPSWAT will exhibit from Stand C55, Hall 7. 

MEA TECHNOLOGY AND BUSINESS LEADERS INCREASINGLY LOOK TO OPSWAT TO DEFEND THEIR IT/OT SUITES. WE STAND READY AS THEIR TRUSTED PARTNER



FORTINET STRENGTHENS AI-POWERED CYBERSECURITY VISION AT GISEC GLOBAL 2025

ALAIN PENEL, VICE PRESIDENT FOR THE MIDDLE EAST, TURKEY, AND CIS AT FORTINET, HIGHLIGHTS AI INNOVATION, EMERGING THREATS, AND THE COMPANY'S DRIVE TO BUILD COLLECTIVE CYBER RESILIENCE.

Cybersecurity is undergoing a major transformation, driven by the rapid evolution of AI, quantum computing, and increasingly complex threat landscapes. At GISEC Global 2025, Fortinet is showcasing how its AI-powered innovations are shaping the future of secure networking and threat intelligence. In an exclusive conversation with CPI Media Group, Alain Penel, Vice President for the Middle East, Turkey, and CIS at Fortinet, shares insights

into the company's regional strategies, collaboration initiatives, and long-term vision for cybersecurity in 2025 and beyond.

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

As today's network complexity grows, so does the need for intelligent tools that can simplify management tasks and enhance efficiency. This year's GISEC

theme is 'Securing an AI-powered future', and at Fortinet, we have pioneered AI innovation within cybersecurity for more than a decade, with AI serving as the backbone to the Fortinet Security Fabric and FortiGuard Labs threat intelligence and security services – it's in our DNA.

For organisations in the Middle East seeking to advance in the realm of AI, we're here to support them in having a clear and comprehensive strategy aligned to their existing business initiatives, providing a partner that is an

expert not only in cyber, but that has a solid understanding of AI's real-world application.

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

In 2025, cybersecurity challenges will evolve to become even more complex. Threat actors are becoming more specialized, especially in the early stages of attacks, focusing on reconnaissance and weaponization.

Cybercrime-as-a-Service (CaaS) for example is expanding, making advanced tools like phishing kits and automated hacking solutions widely available, even to less skilled attackers. The increasing reliance on multi-cloud environments also introduces more vulnerabilities, creating a larger attack surface for cybercriminals. What's particularly concerning is the convergence of physical and digital threats, where cyberattacks are paired with real-life intimidation tactics targeting executives and employees.

The use of AI and quantum computing will also transform the threat landscape. Cybercriminals are already using AI to automate reconnaissance and streamline phishing attacks, and this trend will only grow. On the flip side, AI offers promise for real-time threat detection and response. Quantum computing, while still in its early stages, could disrupt traditional encryption methods, making it crucial for businesses to adopt post-quantum cryptography to protect sensitive data. These technologies highlight the need for businesses to stay ahead of the curve and rethink their cybersecurity strategies.

Can you highlight any innovative technologies or solutions your company is showcasing at this year's event?

At this year's GISEC we'll be showcasing our SASE and Zero Trust solutions and how they can help each organisation pave a path to a safer network. Of course, we'll also be showcasing our leading AI-Powered Security Operations and how we are uniting intelligence with visibility, automation, and protection.

Our commitment to AI innovation is reflected in our expansion of generative AI, which now enhances seven different products across our portfolio. By integrating FortiAI in such a broad range of solutions, we're equipping our customers with powerful, adaptive tools that transform how they manage and respond to cyberthreats, enabling IT and security teams to better secure their organizations. You can learn more from our experts at the event.

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

At Fortinet, we believe our corporate responsibility is to make the world a safer place, creating a digital world you can always trust. Working across sectors and prioritizing threat intelligence sharing benefits the cybersecurity community, making us more resilient and effective collectively.

That's why we are committed to partnership and cooperation with global law enforcement agencies, government organizations, and industry organizations. As the global cybercrime landscape evolves, these collaborations will only become more critical to halting threat actors. When we work together, we

can move faster and more effectively toward our collective goal of disrupting cybercrime.

Fortinet is also proud to be part of numerous collaborative efforts to address cybercrime, such as being a founding member of the World Economic Forum Centre for Cybersecurity, a contributor to its Partnership Against Cybercrime (PAC), and a founding member of the Cybercrime Atlas, which meets weekly to profile threat actors, review open-source intelligence regarding cybercriminal activities, correlate data, and identify potential disruption points.

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

Our commitment to AI-driven security innovation in 2025 and beyond remains stronger than ever. We will continue enhancing FortiGuard AI-Powered Security Services to analyze real-time threat intelligence, strengthening defenses against known, unknown, and AI-driven cyberthreats. FortiAI Ops will further evolve its machine learning capabilities to provide even more predictive insights, enabling IT teams to proactively manage performance and security. FortiAI will expand its generative AI capabilities to streamline security operations, automate investigations, and improve threat response across more of our solutions. And we will advance our AI-powered DLP to better prevent data leaks and unauthorized AI access, ensuring compliance and safeguarding sensitive information.

Our focus will also remain on capturing our massive opportunities across secure networking, unified SASE, and security operations. Moving forward, we aim to drive further enterprise adoption and reinforce our leadership in these critical areas. Additionally, Fortinet was recently recognized on the Forbes Most Trusted Companies in America list, ranking seventh overall and the only cybersecurity company in the top 50. This recognition reflects our commitment to transparency, security, and customer trust. 🔒

FORTIAI WILL EXPAND ITS GENERATIVE AI CAPABILITIES TO STREAMLINE SECURITY OPERATIONS, AUTOMATE INVESTIGATIONS, AND IMPROVE THREAT RESPONSE ACROSS MORE OF OUR SOLUTIONS.



**Maher Jadallah, Vice President,
Middle East & North Africa, Tenable.**

TENABLE TO HIGHLIGHT HOLISTIC APPROACH TO CYBER EXPOSURE



Tenable, the Exposure Management company, will showcase Tenable One Exposure Management Platform - the world's only AI-powered exposure management software

from booth C175 in Hall 5 at GISEC Global 2025 at the Dubai World Trade Centre from 6 - 8 May.

"Over the past seven years, Tenable has undergone a significant strategic evolution, methodically expanding its capabilities across Identity Security, Cloud Security, Operational Technology (OT), Attack Path Analysis and Exposure Analytics," said Maher Jadallah, Vice President, Middle East & North Africa, Tenable.

"Scattered products and siloed views have left organisations struggling to hold back threats across a fragmented attack surface. We know the war against cyber risk can be won with holistic security strategies and solutions. At GISEC we'll be showing organisations how they can regain control of their environments to reduce their risk and end their exposures."

Effective exposure management requires a unified view of the entire attack surface, allowing security teams to detect toxic risk combinations, identify attack path choke points and prioritise weaknesses based on their true impact on the organisation. Tenable One radically unifies security visibility, insight and action across the attack surface, equipping modern organisations to isolate and eradicate priority cyber exposures from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. 🔑

"OVER THE PAST SEVEN YEARS, TENABLE HAS UNDERGONE A SIGNIFICANT STRATEGIC EVOLUTION, METHODICALLY EXPANDING ITS CAPABILITIES ACROSS IDENTITY SECURITY, CLOUD SECURITY, OPERATIONAL TECHNOLOGY (OT), ATTACK PATH ANALYSIS AND EXPOSURE ANALYTICS. MAHER JADALLAH, VICE PRESIDENT, MIDDLE EAST & NORTH AFRICA, TENABLE"



Meriam ElOuazzani, Senior Regional Director, META, SentinelOne.

SENTINELONE TO SPOTLIGHT AI-POWERED CYBERSECURITY AT GISEC 2025

SentinelOne, a global leader in AI-powered security, announces its participation at GISEC Global 2025 (6-8 May) at the Dubai World Trade Centre. The company will highlight how AI-driven cybersecurity is transforming threat detection, response, and prevention across enterprise, and showcase its Singularity Platform, an AI-powered solution that brings together endpoint, cloud, and identity security in a single, cohesive platform.

SentinelOne will also present Singularity Hyperautomation, which enables security teams to connect, automate, and accelerate workflows without writing a single line of code. Moreover, purpose-built for the autonomous SOC, SentinelOne's AI-SIEM will also be on display, delivering real-time, exabyte-scale analytics using adaptive models that go beyond static rules to detect and respond to threats instantly.


A recent report by the UAE Cyber Security Council and CPX highlights that over 223,800 assets hosted within

the UAE are potentially vulnerable to cyber-attacks, with half of the critical vulnerabilities remaining unaddressed for over five years. Misconfigurations account for 32% of these incidents, followed by improper usage and unlawful activities at 19%. Sectors such as government, finance, and energy are identified as primary targets for malicious actors. The financial implications are equally concerning, with the Middle East recording the second-highest data breach costs globally. Additionally, the region has witnessed a 58% increase in ransomware activity, underscoring the escalating risk landscape.

"Digital transformation across the Middle East has expanded attack surfaces, exposing organizations to increasingly sophisticated cyber threats," said Meriam ElOuazzani, Senior Regional Director, META, SentinelOne. "With ransomware on the rise and critical vulnerabilities left unpatched for years, traditional security is no longer enough. Our unified, AI-powered platform helps organizations

modernize their defenses, cut response times, and stay ahead of today's evolving threat landscape. GISEC is not just a trade show us; it is a launchpad for innovation, partnerships, and leadership."

Returning to GISEC, Purple AI brings enhanced capabilities – natural language prompts, automated investigations, and smart summaries – that streamline threat detection and amplify analyst productivity, while ensuring data privacy. SentinelOne will also demonstrate Singularity Cloud Security for real-time protection across hybrid environments, and Identity Threat Detection & Response (ITDR) which defends against identity-based attacks with autonomous detection and rapid remediation across Active Directory and Azure AD.

Senior executives from SentinelOne will host live demos, expert-led sessions, and interactive experiences at Stand C110 in Hall 6. Attendees can participate in "Mortal vs. Machine," a unique experience that pits human analysts against SentinelOne's AI platform, showcasing AI-driven security's unmatched speed and accuracy. Visitors to the booth can experience firsthand how these solutions empower security teams to detect, investigate, and respond to threats faster – all with greater precision. 

"DIGITAL TRANSFORMATION ACROSS THE MIDDLE EAST HAS EXPANDED ATTACK SURFACES, EXPOSING ORGANIZATIONS TO INCREASINGLY SOPHISTICATED CYBER THREATS"

CPX RETURN TO GISEC SPOTLIGHTS UAE CYBER LEADERSHIP AND INTERNATIONAL GROWTH



Hadi Anwar, CEO of CPX.

CPX Holding, a leading provider of cutting-edge cyber and physical security solutions and services, will participate at GISEC Global 2025 for the third consecutive year, marking its biggest presence yet at the region's leading cybersecurity event.

Taking place from 6–8 May 2025 at the Dubai World Trade Centre, GISEC Global brings together global cybersecurity stakeholders to address the evolving threat landscape and unlock

new opportunities for resilience and innovation.

"GISEC has become a key global platform for shaping the future of cybersecurity," said Hadi Anwar, CEO of CPX. "For CPX this year, it will be a key moment that demonstrates the strength of our partnerships, the depth of our expertise, and our growing role in safeguarding digital ecosystems in the UAE and beyond. During GISEC, we will also be announcing several key milestones that reflect our ongoing

commitment to building a secure, inclusive, and AI-empowered digital future. We're proud to return for the third year in a row—not just to showcase innovation, but to drive meaningful conversations around security, readiness, and collaboration."

The theme of this year's participation is Experience the Power of Cyber Innovation, to empower organizations with cutting-edge, end-to-end cybersecurity solutions that are tailored to confront today's most advanced threats. CPX will exhibit at booth A30 (between Halls 7 and 8), hosting a lineup of international technology partners and showcasing its comprehensive portfolio of cybersecurity solutions designed to protect digital environments across the public and private sectors. This year's participation comes as CPX accelerates its international expansion, reinforcing its role as a trusted national champion with a growing global impact.

The CPX booth will feature confirmed partner pods from: Palo Alto, Rilian Technologies, Corelight, Fortinet, Thales, Goteleport, Mindflow, Splunk, and Cribl. Visitors can explore the CPX booth to learn more about its cybersecurity offerings, experience partner technologies, and hear from experts shaping the future of secure digital transformation.

CPX will also be taking part in several center-stage speaking engagements on the main stage panel discussion as part of GISEC's Government Track. Titled "Cyber Resilience and Data Protection in the Cloud Age", the session will explore how organizations can strengthen cloud defenses amid rising threats, with 83% of workloads expected to run in the cloud by 2025. 📌



INFOSEC & CYBERSECURITY

CONGRESS 2025

Securing the Intelligent Age

5th May 2025

AI Habtoor Grand Resort,
Autograph Collection, JBR

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 **5th May 2025** at **AI Habtoor Grand Resort, Autograph Collection, Dubai**, and be part of the movement shaping the future of secure digital transformation.

CYBER RESILIENCE STRATEGIC PARTNER



GOLD SPONSORS



OFFICIAL PUBLICATIONS



HOSTED BY



#infosec&cybersecuritycongress2025 | #tahawultech | #isacauaechapter

Niraj Tolia, Chief Technology
Officer at Veeam.



**SECURITY STARTS WITH MANAGING YOUR
USERS AND ENSURING THE RIGHT PEOPLE
HAVE ACCESS TO THE RIGHT SYSTEMS. THAT'S
→ WHY PROTECTING ENTRA ID IS SO IMPORTANT,
AND WHY IT'S THE LATEST ADDITION TO OUR
VEEAM DATA CLOUD PLATFORM**

VEEAM DATA CLOUD FOR MICROSOFT ENTRA ID BRINGS EFFORTLESS DATA RESILIENCE TO PROTECT AND SECURE IDENTITY MANAGEMENT

NEW ENTERPRISE-READY SAAS SOLUTION SIMPLIFIES THE PROTECTION OF ORGANIZATIONS' MICROSOFT ENTRA ID USERS

Veeam Software, the #1 leader by market share in Data Resilience, announced today the launch of Veeam Data Cloud for Microsoft Entra ID.

With Entra ID (formerly Azure AD) facing over 600 million attacks daily, protecting organizations' digital identity has never been more critical. Veeam Data Cloud for Microsoft Entra ID is a Software-as-a-Service (SaaS) backup solution designed to simplify data resilience for Entra ID tenants, ensuring organizations can protect their essential assets.

Support for Entra ID is the latest extension of Veeam Data Cloud, a powerful, unified and intuitive cloud platform. Delivered with the simplicity of SaaS, Veeam Data Cloud integrates modern cloud-native technologies and AI acceleration to protect, secure, and manage data on-premises and in the cloud to enhance business continuity and usability while driving greater efficiencies.

"Security starts with managing your users and ensuring the right people have access to the right systems. That's why protecting Entra ID is so important, and why it's the latest addition to our Veeam Data Cloud platform," said Niraj Tolia, Chief Technology Officer at Veeam. "We are giving customers greater simplicity with an enterprise-ready, pre-hardened, and self-configured SaaS solution that removes the burden of managing

and maintaining complex backup infrastructure."

Protecting Entra ID includes not only addressing cybersecurity threats, but also managing compliance requirements, recycle bin limits, accidental deletions, and policy misconfigurations. Veeam Data Cloud for Microsoft Entra ID offers comprehensive backup and restore capabilities for Entra ID users, groups, application registrations, and other objects, providing an all-in-one cloud service with unlimited storage and a unified UI for a streamlined user experience. With Veeam Data Cloud for Microsoft Entra ID, organizations can maintain data resilience and quickly recover from issues affecting Entra ID.

Key features of Veeam Data Cloud for Microsoft Entra ID include:

- **Proactive Protection:** Enhances visibility and control over changes within Entra ID, ensuring business continuity, security, and compliance.
- **Effortless Recovery:** Allows quick restoration of Entra ID users, groups, attributes, app registrations, logs, related metadata, and more with reliability.
- **Comprehensive Inclusion:** Offers a secure backup service managed by experts, offloading maintenance, updates, and security fixes.

"Protecting Microsoft Entra ID

has never been more important. In fact, one in five respondents in Futurum's Cybersecurity Decision Maker IQ research indicated credential compromise/account takeover as a security incident most impacting their organization. Veeam is making resiliency for these environments, including visibility into potentially malicious behavior and automated backup jobs, accessible to a broader range of customers by delivering it in a managed and hosted model with the addition of Entra ID protection to Veeam Data Cloud." said Krista Case, Research Director at The Futurum Group.

Veeam Data Cloud already provides businesses with the ability to protect Microsoft 365 workloads and with the latest addition of Entra ID, existing customers can bundle Veeam Data Cloud for Entra ID with their existing Veeam Data Cloud for Microsoft 365 Flex and Premium investments to continue to only pay per Microsoft 365 user.

As part of Veeam Data Cloud, customers can manage all their workloads across a single interface, extending the platform's comprehensive features to Entra ID and future workloads. These include advanced security controls such as role-based access control, reduced complexity, and streamlined reporting, all while offloading maintenance, updates, and security fixes. 🔒

HOW AI IS REINVENTING CYBERSECURITY FOR THE AUTOMOTIVE INDUSTRY

I AI IS ACCELERATING THE MIDDLE EAST'S JOURNEY TOWARD CONNECTED MOBILITY — BUT ONLY CYBER-SECURE INNOVATION CAN ENSURE A SAFE AND SUSTAINABLE RIDE INTO THE FUTURE.

Autonomous and electric vehicle uptake is rising across the Middle East, driven by national agendas and a growing push for sustainable mobility. With this rapid growth however comes an urgent need to address cybersecurity at every stage of the automotive value chain.

Artificial Intelligence (AI) is at the heart of this shift; transforming not only how vehicles operate, but also how cyber threats are identified, mitigated, and prevented. From predictive maintenance to driver behavior analytics, AI is streamlining processes and unlocking efficiencies. But it is also redefining the security perimeter for automotive organizations.

Forces Influencing AI Adoption in Automotive

As the industry evolves, three forces are shaping the current landscape: stricter regulations, rapid AI integration, and a fundamental change in communication infrastructure. Regulations such as the Cyber Resilience Act and NIS2 for

example are introducing more granular compliance mandates, especially for sectors handling critical infrastructure.

Meanwhile, AI is accelerating business and individual learning processes. At the network level, the need for faster communication and bandwidth adaptability is giving rise to next-generation connectivity frameworks that can support AI-native systems.

This evolution in infrastructure and intelligence also promotes a significant shift in cybersecurity from reactive to preventive. AI is increasingly being used to analyze threat landscapes and internal vulnerabilities in real-time. This shift enables organizations to prepare for attacks before they happen, leveraging behavioral analytics and high-speed correlation to stay ahead of potential breaches. Hardware acceleration and software development, guided by AI, are now setting the pace for how cybersecurity evolves across the industry.

The Impact of Cybersecurity

Unsurprisingly, automotive enterprises are becoming high-value targets for

cybercriminals. Three core factors contribute to this trend; the financial opportunity of holding connected services hostage, the complexity of digital supply chains, and the vast amount of sensitive data being generated.

With every vehicle connected to cloud-based services, a single breach can have wide-ranging brand, operational, and financial repercussions. Moreover, the ecosystem of third-party vendors involved in producing autonomous and electric vehicles significantly expands the attack surface.

The use of digital twins and advanced manufacturing technologies further intensifies the volume of valuable data. This information ranging from user behavior patterns to proprietary designs is not only attractive to attackers but also becomes a tool for launching future attacks or selling on the dark web.

AI Transformations in the Automotive Supply Chain

AI is also transforming the automotive supply chain. Predictive maintenance for example – as opposed to scheduled or reactive vehicle maintenance, which until now has been the norm – enables companies to forecast part failures, optimize distribution, and reduce warehousing costs. AI can analyse and synthesise so many data streams that this guessing game becomes much more

“WITH EVERY VEHICLE CONNECTED TO CLOUD-BASED SERVICES, A SINGLE BREACH CAN HAVE WIDE-RANGING BRAND, OPERATIONAL, AND FINANCIAL REPERCUSSIONS”



**Alain Penel, Vice-President,
Middle East, Turkey, and CIS at Fortinet.**

accurate. Not only does this mean more reliable vehicles for the consumer, but it also means that each element of demand can be optimised.

Driver behavior analysis and in-cabin monitoring systems powered by AI are also enhancing safety, particularly for long-haul truck drivers exposed to risks such as fatigue and theft. These AI-powered innovations are already helping companies reduce operational costs while improving customer satisfaction.

Strengthening security across the supply chain means embedding real-time monitoring, mapping data flows, and building a fast, coordinated response to incidents. The introduction of cyber resilience principles encouraged by regulatory bodies requires organizations to maintain robust and sustainable response mechanisms. AI can help with this.

AI's Role in Automotive Cybersecurity

The future of AI in automotive cybersecurity lies in its ecosystem-wide integration. Multimodal AI models that can process text, images, and design data are already in use.

But the next phase involves combining internal and external intelligence to strengthen risk postures. Synthetic data created specifically to train internal models without exposing real user data is becoming an important asset in speeding up AI development while preserving privacy.

The impact of AI can be summarized as transformative, dual-edged, and adaptable. It is enhancing cybersecurity readiness, being weaponized by attackers, and empowering businesses to evolve quickly in a changing environment.

As the Middle East embraces connected mobility and smart transportation, the conversation must move beyond adopting AI to implementing it securely and intelligently. The road to the future may be autonomous, but its success will hinge on cybersecurity built for adaptability, speed, and scale. 📌

THE IOT IMPERATIVE - SECURING TODAY'S CRITICAL INFRASTRUCTURE



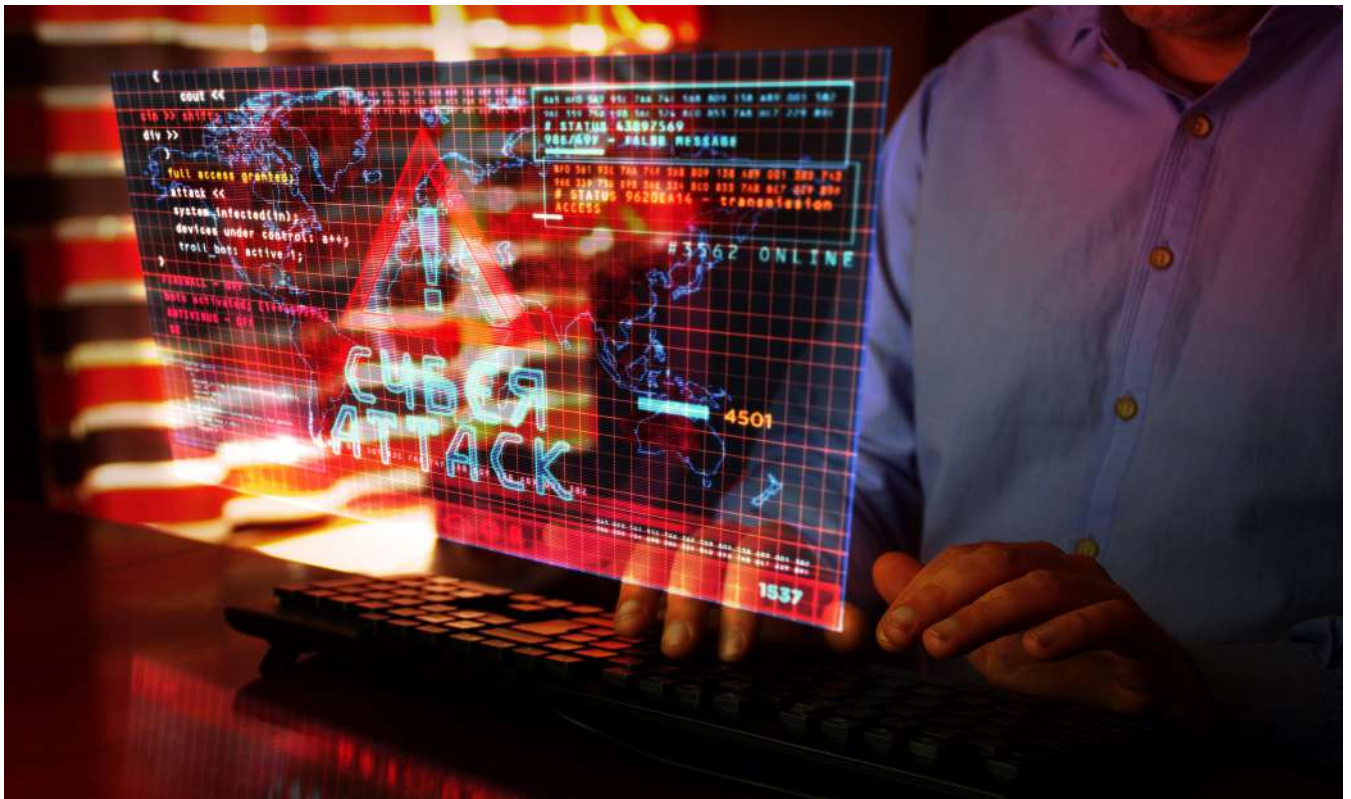
Michael Dugent, IoT Director, EMEA
at Nozomi Networks.

Digitalization has accelerated across nearly every aspect of society and millions of new devices are being integrated into corporate networks and the internet daily, dramatically expanding the attack surface for malicious actors.

Cybersecurity experts highlight that many modern attacks are driven by a desire for control and destruction, making critical infrastructure a prime target for hackers. Critical infrastructure systems - the assets and networks, be they physical or virtual, underpinning the functioning of an economy and society - determine the security, prosperity, well-being, and resilience of an entire nation.

A recent report focused on Operational Technology (OT) and Internet of Things (IoT) security, revealed that threat actors are not only escalating their attack frequency but also honing their tactics and identifying new entry points. In 2023, cyberattacks fueled by nation-state actors affected 120 countries, with over 40% targeting critical infrastructure.

Nowadays, cyberattacks on critical infrastructure represent a global risk, demanding heightened attention and a deeper understanding of activities that pose a potential threat.



Attacks on critical infrastructure environments often include targeting IoT environments first, as these devices are often easier to compromise and monitoring of these environments is still limited. In this regard, IoT is an important concept embedded within a larger spectrum of networked products and digital sensors that has caused an explosion of applications, marking a fundamental shift in the way human beings interact with the Internet, amplifying both opportunities and challenges surrounding critical infrastructure across the globe. The question arises: why do threat actors target IoT environments?

In October 2016, the most significant DDoS attack in history left a large portion of the East Coast of the United States without internet. The following year, hackers accessed sensitive personal and financial data from a North American casino. In March 2021, a security camera company was attacked, exposing live feeds from 150,000 surveillance cameras

in hospitals, manufacturing facilities, prisons, and schools. The common thread among these three attacks was that the perpetrators targeted the IoT environments of these companies to gain access to their internal systems.

The Internet of Things, known as IoT, is a system of interconnected computing devices. The definition of what constitutes an IoT device varies widely and includes everything from biomedical implants to sensors on manufacturing and electrical equipment. An industrial ecosystem can encompass many different smart devices that collect, send and act on data from their environments. Sometimes, these devices even communicate with each other and act on the information they get from one another.

Over the last 10 years, industrial and critical infrastructure operators have rapidly deployed billions of devices to optimize their automation processes using the data provided by these "things". Unfortunately, this

trend has created new cybersecurity risks, as these devices are open to networks, both public and private. These endpoints have become low-hanging fruit for attackers who want to compromise operational processes and maximize the economic benefits of a cyberattack.

As digital transformation leads to an increase in unmanaged devices across industrial environments, the importance of a robust IoT security program to safeguard critical infrastructure from cyberattacks cannot be overstated. But what makes IoT security such a challenge for companies?

First of all, IoT devices are often unmanaged and inherently insecure. Once deployed, the software on these devices is seldom updated, especially firmware where many vulnerabilities exist. As a result, these devices remain susceptible to attacks that could easily be prevented on other managed devices. Secondly, the use of default passwords and weak authentication

procedures makes these devices easier to compromise than managed IT devices. Attackers frequently exploit default and predictable passwords to access smart devices, which can then be used to target other critical devices and networks. Recent regulations announced by the UK Government aim to address this issue by banning manufacturers from using weak, easily guessable default passwords. But while this is a significant step towards eliminating ‘insecure by design’ devices, it is not enough to protect IoT environments from penetration.

Another reason for IoT environments having weak resilience is that IoT devices typically connect to an ecosystem that includes business applications, data centers, IT infrastructure, and the cloud. Their inherent lack of robust cybersecurity controls makes them attractive targets for hackers seeking entry into broader networks. Moreover, large-scale industrial IoT deployments do not easily accommodate the level of network segmentation required to mitigate cyber threats or prevent malware spread. Most IoT devices also lack the capacity to host software security agents due to their limited processing and communication capabilities, as well as insufficient space for such software.

Finally, IoT devices are often deployed without the involvement of IT or cybersecurity teams. This can lead to devices being placed in sensitive or insecure areas of the network, making them easier to compromise due to the absence of additional cybersecurity layers.

Companies operating critical infrastructure must adhere to certain OT and IoT security guidelines and best practices to mitigate cyber risk.

First, it’s essential for companies to understand the types of IoT devices used within their organization and the associated risks, and to make sure that every device is accounted for. This involves identifying all of the devices communicating on the

network (including devices connected wirelessly), understanding the data these devices collect and transmit, and understanding the potential impacts of a cybersecurity incident. An integral part of this step is implementing an asset management mechanism that can track every connected device with real-time data.

Second, organizations should take steps to protect their networks from threats by deploying suitable security controls. This includes measures capable of isolating or terminating connections linked to malware or other anomalies. It also encompasses

network segmentation, multi-factor authentication (MFA), and encryption. Companies should establish a process to understand the most critical assets and to prioritize patching the highest risk and most vulnerable assets first to reduce overall risk exposure and increase resilience.

Implementing monitoring and detection mechanisms is another crucial step for companies to identify potential cybersecurity threats and vulnerabilities. These mechanisms could involve network monitoring, log analysis, and security incident and event management (SIEM) systems. Utilizing an industrial



network monitoring solution that integrates with network access control (NAC) products can expose significant potential risks in real-time.

Next, companies need to develop a plan for responding to cybersecurity incidents. This includes procedures for isolating affected devices and systems and communicating about the incident to relevant parties. Comprehensive incident response playbooks and forensic analysis tools can aid in achieving this swiftly and efficiently. Finally, planning and practicing business continuity strategies for recovering from cybersecurity incidents

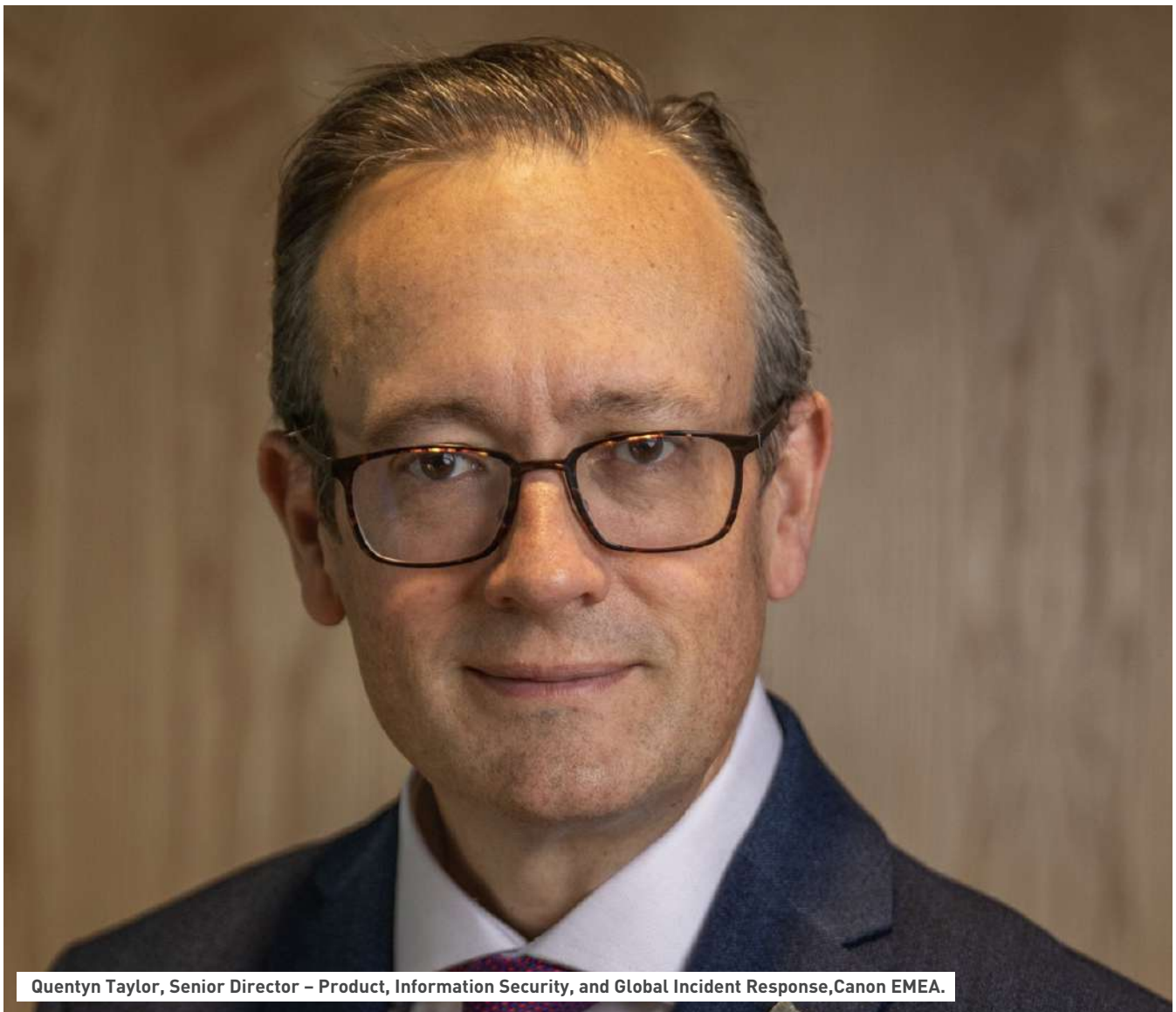
is vital. This includes procedures for restoring affected systems and processes and mitigating any potential impacts.

In addition to these steps, companies should collaborate with industry partners and government agencies to share information about cybersecurity threats affecting IoT devices. Regularly reviewing and enhancing cybersecurity procedures to ensure they remain effective against the evolving threat landscape is also recommended. Critical infrastructure organizations should prioritize proactive defense strategies that include network

segmentation, asset discovery, vulnerability management, patching, logging, endpoint detection, and threat intelligence. There is also a growing need for actionable asset and threat intelligence that can be used by different stakeholders within an organization such as IT teams, compliance officers and risk managers who may have different perspectives on security issues.

Ultimately, securing IoT devices within critical infrastructure is non-negotiable in maintaining national stability, operational continuity, and safeguarding the interconnected systems that support our way of life. 📌

FORTIFYING CYBER SECURITY: WHAT DOES SECURE LOOK LIKE IN 2025?



Quentyn Taylor, Senior Director – Product, Information Security, and Global Incident Response, Canon EMEA.

The scale that the cybersecurity landscape has changed in recent years has led to increasing pressures for IT leaders. With the World

Economic Forum estimating the global cost of cybercrime is projected to reach \$10.5 trillion annually in 2025, the situation is only expected to become more challenging.

Now, to meet this ongoing challenges, IT leaders of 2025 are likely to spend more time and energy on maintaining information security, with Canon research finding that today half (50%) already name this as one of their top three most time-consuming responsibilities. In fact, security has been reported as a top concern, with leaders consistently ranking it as one of the most challenging aspects of their roles since 2019.

With the threat landscape evolving at an unprecedented pace, prompted by evolutions in AI maintaining IT security can feel like a constantly moving target. However, while AI poses new challenges, businesses must not lose sight of the basics of a robust security strategy, and ensure compliance stays front and centre with incoming security regulations in the year ahead.

The new AI reality

There are a wealth of new and evolving technologies, which include those powered by AI, which provide even more opportunities for cybercriminals to attack.

AI's ability to enhance the scale and sophistication of attacks means IT infrastructure needs to withstand an increasing number of threats. For example, cyber criminals are using AI to carry out more sophisticated phishing attacks, through leveraging personalisation and deep fakes to increase their effectiveness. Phishing attempts are being made more convincing through auto translation, enhanced targeting, localisation and in some cases even audio creation.

While the AI threat may seem daunting, AI is still yet to be used by attackers on a large scale simply because tried and tested methods are still proving effective.

As such, a crucial part of the solution lies in strengthening a business' first line of defence – its people. Ensuring employees are effectively trained and have the skills to spot and report phishing attempts can act as a critical defence against preventing an attack. By establishing better security awareness across the organisation, businesses will be better prepared to deal with both the threats of today and the AI-powered attacks of tomorrow.

Mastering the basics

Robust information security policies have always been important, but in the age of AI, extra vigilance to threats is essential. Now more than ever, ensuring that you foster a culture of good cyber hygiene will make it harder for AI-driven threats to penetrate through company lines.

Paying constant attention to the basics could make all the difference, ensuring the right foundations to build a comprehensive and robust cybersecurity strategy. A significant number of the high-profile incidents that have occurred in the past couple of years have not been from overly sophisticated avenues, but instead through tried and tested methods, for example unpatched software vulnerabilities. This means taking into consideration key building blocks such as managing the perimeter of a company, multi-factor authentication (MFA), regular updates and security patches, and a robust recovery action plan, can go a long way to keeping away would be attackers.

Embracing MFA and prioritising a high level of employee education will be crucial foundational elements in building defences against AI-powered threats of the future. To meet new cyber challenges MFA is evolving. From numbers on a screen to leveraging the power of a mobile phone and data connection, advanced capabilities are helping to combat man in the middle attacks through comprehensive identity verification via location verification and access pattern analysis.

While ensuring that good cyber practices are the enforced default with MFA and automated updates, educating employees

on how to work in a secure way and building security awareness throughout the organisation is crucial and may be the difference between a contained threat and a costly cyber incident.

The regulation revolution

In recent years, national governments have intensified efforts to address evolving threats and bolster cyber resilience. Businesses are welcoming this renewed support from governments for standardisation. Not only does this strengthen security within individual businesses, but it also bolsters confidence in third party software and hardware, through the creation of standardised procedures and common information security frameworks. Furthermore, continuing conversations around how to regulate against the threats posed by the age of AI, businesses should ensure they remain compliant not only now, but well into the future.

Now, IT leaders must reevaluate their cybersecurity strategy to meet the requirements of today and those of the future. They must make considered and meaningful decisions on software and hardware procurement to ensure they are prepared for a landscape of more rigorous regulation.

Preparing for future threats

As we witnessed in 2024, the security landscape is becoming increasingly nuanced and complex and this isn't set to change in 2025. The rise of AI has not only intensified but also significantly advanced the sophistication of attacks, while an evolving regulatory environment adds further complexity. In this context, cybersecurity must remain front and centre for IT leaders.

In an era of advanced threats, the importance of mastering the basics can be overlooked, yet it plays a crucial role in preventing attacks. Organisations that continue to prioritize these basics will strengthen their cyber resilience in 2025, positioning themselves to effectively navigate any challenges that arise in the next couple of years. 🧑

COHESITY UNVEILS NEW NETBACKUP FEATURES AND NUTANIX INTEGRATION

NEW RELEASE INCLUDES QUANTUM-PROOF ENCRYPTION, ENHANCES INDUSTRY-FIRST USER BEHAVIOR MONITORING AND RISK ANALYSIS, AND ADDS PROTECTION FOR MORE PAAS WORKLOADS

Cohesity, the leader in AI-powered data security, announced multiple new features for Cohesity NetBackup 11.0 to help organizations protect against current and future cyber threats. The new capabilities reflect the company's continued commitment to, and investment in, the NetBackup data protection solution, providing customers with data security innovations such as quantum-proof encryption, advanced analytics to identify high-risk user behavior, and support for more PaaS workloads.

"This represents the most powerful NetBackup software release to date for defending against today's sophisticated threats and preparing for those to come," said Vasu Murthy, senior vice president and chief product officer, Cohesity.

"Securing a modern data estate can be increasingly challenging for organizations, especially as cybercriminals evolve their attack methods. Defense strategies must also evolve. The latest NetBackup features give customers smarter ways to minimize the impact of attacks now and post-quantum."

NetBackup 11.0: Strengthening Data Security and Cyber Resilience

NetBackup release 11.0 is available globally. Feature benefits include:

- Quantum-proof encryption – guards



Vasu Murthy, senior vice president and chief product officer, Cohesity.

against "harvest now, decrypt later" quantum computing attacks and protects long-term confidentiality across all major communication paths within NetBackup, from encrypted data in transit and server-side dedupe to client-side dedupe and more.

- Broadened user behavior monitoring – monitors for an expanded range

of unusual user actions. This unique capability can stop or slow down an attack, even when threat actors compromise administrative credentials with an intent to destroy data.

- Improved risk scoring – further strengthens the security posture of data by automatically provisioning recommended values for more



security settings. Malicious configuration changes can be stopped by dynamically intercepting suspicious changes with multi-factor authentication.

- Expanded cloud support – protects additional cloud workloads and increases efficiency with shorter backup windows in the cloud. NetBackup has extended PaaS workloads protection to support Yugabyte; Amazon DocumentDB; Amazon Neptune; Azure Cosmos DB (Cassandra and Table API); Amazon RDS Custom for SQL Server and Oracle Snapshots; and Azure DevOps/GitHub/GitLab. NetBackup 11.0 also enables image replication and disaster recovery from cloud archive tiers like Amazon S3 Glacier and Azure Archive.

NetBackup is endorsed by Sheltered Harbor for meeting the most stringent cybersecurity requirements of U.S. financial institutions and other organizations worldwide. Learn more about the new NetBackup 11.0 features.

Enhanced Database Protection Through Nutanix Integration

As part of its ongoing commitment to strengthening cyber resilience, Cohesity has also become the first data protection vendor to achieve Nutanix Database

Service (NDB) database protection Nutanix Ready validation. This validation enables Cohesity DataProtect to integrate with NDB's native time machine capabilities, streamlining protection for PostgreSQL databases on NDB through a single control plane.


"Every second of downtime and byte of data lost has an associated dollar and reputational cost. Large enterprises, particularly those in critical sectors like global banking, financial services, and the Fortune 500, are under nearly constant threat and need solutions that can keep their data safe, reduce or eliminate downtime, and recover critical services quickly," said Murthy.

"Nutanix and Cohesity are trusted by so many organizations because of our

speed, scalability, simplicity, and security. With this integration, we're working closely together to help them safeguard their most critical operations."

By combining Cohesity DataProtect with NDB's native time machine capabilities, customers gain:

- Enhanced security and cyber resilience – objects are safeguarded from being overwritten and protected against deletion for a specified amount of time. The solution is highly resilient and fault-tolerant, using AES-256 and FIPS-compliant encryption for data in flight and at rest.
- Increased efficiency and cost savings – advanced deduplication and compression optimize storage efficiency and reduce data footprints.
- Improved speed and simplicity – scale-out architecture and unlimited scalability improve backup and restore times to meet growing business needs. Customers can streamline operations using Cohesity's single-pane-of-glass management approach.

Cohesity and Nutanix together provide enterprises with a comprehensive solution that enhances IT infrastructure performance, security, and regulatory compliance while improving overall cyber resilience strategies. 

SECURING A MODERN DATA ESTATE CAN BE INCREASINGLY CHALLENGING FOR ORGANIZATIONS, ESPECIALLY AS CYBERCRIMINALS EVOLVE THEIR ATTACK METHODS.

COHESITY AUTOMATION PROVIDES FASTER, MORE COMPREHENSIVE CYBER INCIDENT RESPONSE

I COHESITY RECOVERY AGENT'S AI-POWERED ORCHESTRATION MAKES CYBER RESPONSE AND RECOVERY EASY SO CUSTOMERS CAN RECOVER FROM INCIDENTS FASTER AND WITH MORE CONFIDENCE

Cohesity, the leader in AI-powered data security, announced Cohesity RecoveryAgent, a new AI-powered cyber orchestration solution for Cohesity NetBackup and DataProtect customers. RecoveryAgent automates cyber recovery preparation, testing, compliance, and response, enabling customers to recover from cyber incidents faster. It offers intelligent, customizable recovery blueprints and enables rigorous testing of recovery processes in a non-production environment, giving customers more confidence in their ability to respond to proliferating cyberattacks.

Simplifying Cyber Recovery Through Automation and Intelligence

Modern IT environments are complex, comprising physical, virtual, and cloud-based systems. Responding to cyberattacks requires organizations to navigate this complexity while ensuring data integrity, availability, and regulatory compliance. RecoveryAgent addresses these challenges by generating customizable blueprints that automate

recovery workflows, making cyber recovery response more efficient and adaptable.

With these customizable blueprints, organizations can better prepare for cyber incidents before they happen. RecoveryAgent's intuitive UI allows teams to easily build recovery plans with scripted workflows that automatically integrate critical steps for incident response, such as threat hunting, malware scanning, and instant data restores. Users can rehearse recoveries to prove the blueprint will effectively recover their data in a non-production environment without impacting production applications. This frequent testing helps ensure readiness for real-world incidents.

RecoveryAgent's Agentic AI capabilities allow recovery teams to:

- Rapidly and easily create and edit recovery blueprints with AI assistance for automated testing of cyber impact or disaster recovery
- Manage granular recovery across multiple domains in complex hybrid environments, including on-premises, cloud, PaaS, and containers



- Speed up forensic investigations through automated threat scanning using native tools and best-in-class threat intelligence from Data Security Alliance partners
- Have more confidence in a clean incident recovery with Agentic AI-powered intelligent recovery point recommendations and blast radius analysis of infected files across domains
- Understand the real-world recovery times and how they align with the business SLAs
- Ensure and demonstrate compliance with regulatory and business drivers by implementing standard recovery practices

"Every moment matters to customers experiencing a cyber incident. Having a comprehensive and thoroughly tested incident response plan can be the difference between minimal disruption and massive impact," said Vasu Murthy, Chief Product Officer, Cohesity. "By simplifying and automating every step of the complex cyber recovery process, RecoveryAgent helps customers boost resilience and respond faster with more



confidence to cyber incidents. The world's largest organizations trust Cohesity because we understand the impact of cyber incidents and consistently offer new solutions like RecoveryAgent to help our customers be more confident in their cyber readiness and recovery."

Seamless Integration for Enhanced Cyber Resilience

RecoveryAgent automates time-consuming and manual tasks such as vulnerability scanning, malware scanning, and data classification into a structured blueprint. It can also automate forensics investigation, configuration hardening, and patching when orchestrated on virtual machines that are recovered within the solution. These capabilities are powered by Cohesity's

Data Security Alliance, which integrates with leading security vendors to help security teams become more agile and productive. Additionally, RecoveryAgent enhances Cohesity's existing clean room solution, making activation faster and more intuitive.

"AntemetA has a complex technology infrastructure, and as a result, we need solutions developed with extensive field experience to enable us to be as effective as possible, especially as we are exposed to increasing amount of cyber risks," said Stéphane Colin, CTO, AntemetA. "This is only possible with trusted partners who take time to understand our unique complexity and work with us to ensure our data can be recovered with confidence and our services guarantee the highest level of

resilience, whatever cyber challenges we face. We have a longstanding partnership with Cohesity because it continues to develop solutions like RecoveryAgent, which help us deliver more relevant and effective services. That, in turn, has earned us an equally long-lasting trust from our customers."

RecoveryAgent is the first new offering to emerge from the joint development efforts of Cohesity and Veritas since the companies came together in December. By combining the capabilities of NetBackup Recovery Blueprints and Recommended Recovery Points with AI-powered intelligence and innovation native to DataProtect, RecoveryAgent is an example of the rapid innovation enabled by integrating both companies' technology. It also highlights Cohesity's commitment to simplifying user experiences and enhancing customer confidence in cyber resilience strategies.

RecoveryAgent is currently available to select customers in Tech Preview and is expected to be generally available for NetBackup and DataProtect customers in the second half of the calendar year 2025. 📌

BY SIMPLIFYING AND AUTOMATING EVERY STEP OF THE COMPLEX CYBER RECOVERY PROCESS, RECOVERYAGENT HELPS CUSTOMERS BOOST RESILIENCE AND RESPOND FASTER WITH MORE CONFIDENCE TO CYBER INCIDENTS.

12TH ANNUAL EDITION OF THE BEYONDTRUST REPORT REVEALS RECORD-BREAKING YEAR FOR MICROSOFT VULNERABILITIES



BeyondTrust, the global cybersecurity leader protecting Paths to Privilege, has released its annual Microsoft

Vulnerabilities Report, revealing a record-breaking number of reported Microsoft vulnerabilities in 2024. Despite ongoing security improvements, attackers continue to exploit key weaknesses, particularly those related to privilege escalation and remote code execution. The 2025 report provides an in-depth analysis of data from security bulletins publicly issued by Microsoft throughout the previous year, providing valuable information about vulnerability trends and the evolving threat landscape to help organizations understand, identify, and address the risks within their Microsoft ecosystems.

Key findings from the 2025 report include:

- A total of 1,360 Microsoft vulnerabilities were reported in 2024, marking an all-time high and an 11% increase over the previous record of 1,292 in 2022.
- Elevation of Privilege (EoP) vulnerabilities comprised 40% (554) of all reported vulnerabilities.
- Security Feature Bypass vulnerabilities surged by 60%, increasing from 56 in 2023 to 90 in

2024, increasing the pressure to reduce software vulnerabilities at the design stage through secure coding and threat modeling.

- Critical vulnerabilities across the Microsoft ecosystem continued to decline overall in 2024.
- Microsoft Edge vulnerabilities increased by 17% to 292 total vulnerabilities, including 9 critical vulnerabilities in 2024, compared to zero in 2022.
- Microsoft Azure and Dynamics 365 vulnerabilities plateaued in 2024.
- There were 587 Windows vulnerabilities in 2024; 33 were critical.
- Windows Server had 684 vulnerabilities in 2024; 43 were critical.
- Microsoft Office vulnerabilities nearly doubled from 2023, reaching 62 in 2024.

Although the total number of vulnerabilities has risen, the longer-term trend shows the pace of growth appear is stabilizing. This, combined with the continued downward trend toward fewer critical vulnerabilities, suggests Microsoft's security initiatives and improvements in the security architecture of modern operating systems are paying off.

However, while vulnerability growth appears steady, the report also highlights the complexity of securing today's vast and diverse ecosystems, where evolving technologies, features, and interdependencies continue to introduce risk.

"THIS YEAR'S DATA OFFERS A CLEAR REMINDER THAT THE THREAT LANDSCAPE ISN'T SLOWING DOWN—IT'S RAPIDLY EVOLVING"



Key predictions and takeaways from this year's report include:

- Unpatched systems remain an easy target, opening the door for widespread exploitation.
- Microsoft's expanding tech stack, including cloud and AI services, will continue to introduce new attack surfaces.
- Novel vulnerabilities will emerge as attackers find new and creative ways to bypass defenses.
- Patches alone are insufficient—they can fail or introduce stability risks, underscoring the need for layered defenses.
- Threat actors are shifting tactics, increasingly targeting identities and privileges over traditional exploits.

Despite the changing threat landscape, some security fundamentals remain unchanged:

- 1) Software vulnerabilities are as inevitable as death and taxes
- 2) Enforcing least privilege remains one of the most effective strategies to reduce risk—even against zero-days and reverse-engineered patches

- 3) Defense-in-depth strategies that combine prevention with detection and response offer the strongest protection—including against modern, identity-based threats.

"This year's data offers a clear reminder that the threat landscape isn't slowing down—it's rapidly evolving," said James Maude, Field Chief Technology Officer at BeyondTrust. "The sustained dominance of Elevation of Privilege vulnerabilities highlights how valuable privileges are to attackers and why they will continue to target identities with privileges to move laterally and gain access to critical systems. These trends reinforce the need for organizations to focus not just on patching, but on securing the underlying Paths to Privilege™ across their environments to reduce the attack surface of every identity and point of access."

The BeyondTrust Microsoft Vulnerabilities Report serves as a trusted resource for organizations to better understand the Microsoft vulnerability landscape, prioritize patching strategies, and strengthen their identity security posture against modern threats. 

ACCELERATING INDIA: TCS LAUNCHES NEXT-GEN CAPABILITIES TO POWER THE COUNTRY'S AMBITIONS TOWARD LEADERSHIP IN DEEP-TECH

I TCS INTRODUCED TCS DIGIBOLTTM, AN AI-ENABLED LOW-CODE PLATFORM, AND ITS GLOBALLY TRUSTED TCS CYBER DEFENSE SUITE IN INDIA, EMPOWERING ENTERPRISES TO FAST-TRACK THEIR DIGITAL INNOVATION AND CYBER RESILIENCE

Tata Consultancy Services (TCS), a global leader in IT services, consulting, and business solutions, is doubling down on its commitment to India's digital growth, with the launch of three India-focused offerings that are sovereign by design, secure by default, and sustainable for the future. Designed to accelerate India's AI-led transformation, TCS has launched TCS SovereignSecure Cloud, TCS DigiBOLT, and TCS Cyber Defense Suite.

This launch marks the beginning of many such offerings tailored for India's unique needs, as TCS dedicates itself to supporting the country's mission of building robust digital solutions that are made in India, for India – and are ready for the world.

The launch took place in New Delhi at TCS' Accelerating India event, attended by marquee public and private sector clients, alongside TCS Chief Executive Officer and Managing Director K Krithivasan, Girish Ramachandran, President –Growth Markets, and other senior TCS leaders.

Girish Ramachandran, President – Growth Markets, said, "India is at an inflection point where data sovereignty, AI, and digital acceleration are converging to create unprecedented opportunities. These new offerings, tailored to India's unique needs,



Girish Ramachandran, President Growth Markets, TCS.

reaffirm our commitment to building a secure, AI-powered digital foundation for India—one that not only safeguards national assets but also fuels innovation, economic growth, and global competitiveness. As India moves towards a new era of digital innovation, TCS will continue to lead with indigenous solutions that empower governments, enterprises, and citizens alike, helping them perpetually adapt in an AI-first era."

The new offerings build upon TCS'

legacy as the digital backbone of India, having powered numerous Digital Public Infrastructure (DPI) initiatives. For over five decades, TCS has been at the heart of India's digital transformation, partnering with the government to deliver critical programs and build robust digital public infrastructure.


TCS SovereignSecure Cloud: Next-Gen Cloud, Nation-First, AI-fuelled:

TCS SovereignSecure CloudTM, is a first-of-its-kind, indigenous and secure cloud built and managed entirely by TCS. This cloud comes with integrated AI capabilities to support government institutions, public sector enterprises, and regulated industries.

TCS DigiBOLTTM: India's Fast Lane to AI-First Transformation: Complementing TCS SovereignSecure CloudTM is TCS DigiBOLTTM, a comprehensive

low-code platform coupled with the power of AI that empowers enterprises to accelerate and scale their end-to-end digital innovation journeys.

TCS Cyber Defense Suite: Global Expertise, Localized Protection:

Security is the cornerstone of this initiative and TCS is introducing its globally trusted TCS Cyber Defense Suite, a security-as-a-service platform, in India, thereby strengthening the cybersecurity framework of enterprises with advanced AI-driven protection. 



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



CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD
CLEANROOM™ RECOVERY



Visit [commvault.com](https://www.commvault.com) to Learn More