60 black hat MIDDLE EAST AND AFRICA MINUTES

black hat MIDDLE EAST AND AFRICA
tahawultech.com

Show dates: 2-4 December 2025, Riyadh Exhibition & Convention Center, Malham, Saudi Arabia
Exhibition hours: 11AM - 8PM

DAY 2

Data-centric security takes centre stage in Saudi Arabia's digital transformation, says top Seclore official

SECLORE'S URAZ FARUKH EXPLORES HOW THE KINGDOM'S REGULATORY DIRECTION AND AI ADOPTION ARE SHAPING THE FUTURE OF COMPLIANCE AND CYBER RESILIENCE.

Saudi Arabia's rapid digital expansion is reshaping how organisations approach governance, risk, and compliance, creating a transformative moment for cybersecurity in the Kingdom. With national regulators strengthening frameworks and enterprises accelerating cloud, AI, and data-driven initiatives, the demand for mature, adaptive, and intelligence-led security models has never been greater. Compliance is no longer viewed as a checkbox exercise — it has become a strategic pillar that supports innovation, sovereignty, and long-term digital resilience.

Within this evolving landscape, Seclore is playing a significant role in helping organisations secure sensitive data across decentralised, multi-cloud, and AI-enabled environments. Speaking to Daniel Sheperd, Online Editor, Tahawultech.com at Black Hat MEA 2025, Uraz Farukh, Vice President Sales – MENA, shared a detailed perspective on Saudi Arabia's cybersecurity maturity, emerging gaps and opportunities, and how Seclore's product strategy aligns with the Kingdom's national digital transformation agenda. Farukh also reflects on the strategic value of Black Hat MEA as a platform for collaboration, customer engagement, and shaping the region's cybersecurity dialogue.

How do you see the Saudi compliance landscape evolving over the next few years?
Saudi Arabia has made tremendous progress in advancing national cybersecurity standards.

Regulators have strengthened guidelines to ensure organisations adopt robust frameworks, enforce data governance, and build resilience against emerging threats. As AI, cloud, and next-generation technologies continue to enter the market, compliance will evolve to accommodate new models of risk and data flow. Organisations will increasingly need to integrate data-centric controls, adaptive security, and continuous monitoring to remain compliant as technologies become more complex. The direction is clear: Saudi Arabia is pushing toward stronger cybersecurity sovereignty while enabling innovation at scale.

What is your assessment of cybersecurity maturity in the Kingdom of Saudi Arabia, and where do you see the most significant gaps or opportunities?
Saudi Arabia has emerged as a regional — and increasingly global — leader in cybersecurity

CONTINUED ON PAGE 3

Forescout outlines OT-IT security priorities as Saudi Arabia accelerates digital industrial transformation and growth

MOHAMMAD TAHMAZ, COUNTRY SALES MANAGER – KSA, DISCUSSES HOW REAL-TIME COMPLETE VISIBILITY WITH ZERO BLIND SPOTS, IN CORPORATE NETWORKS ARE SHAPING THE KINGDOM'S NEXT PHASE OF CRITICAL INFRASTRUCTURE PROTECTION AT BLACK HAT MEA 2025.

Forescout's presence at Black Hat MEA 2025 reflects a pivotal moment for cybersecurity in the Middle East, where OT–IT convergence, smart infrastructure, and giga-project expansion are redefining national risk landscapes. Mohammad Tahmaz, Country Sales Manager – KSA, spoke to Daniel Sheperd, Online Editor, Tahawultech on how real-time complete visibility, automated control, and threat intelligence are becoming essential foundations for securing enterprise environments for both IT and OT infrastructure . Tahmaz's insights highlight the region's growing urgency to safeguard critical infrastructure against increasingly sophisticated adversaries.

What are Forescout's key priorities and focus areas at Black Hat MEA 2025, and how does your presence this year reflect the region's growing urgency around OT security?
Our focus at Black Hat MEA 2025 is centred on raising awareness around OT security and demonstrating how organisations can build resilient, real-time defence capabilities across complex hybrid environments. The region is undergoing rapid digital transformation,

and with that comes an urgent need to secure operational environments that were never originally designed for connectivity. We are showcasing how Forescout delivers continuous visibility, automated control, and risk-based response across OT, IT, IoT and IoMT ecosystems—capabilities that are now essential as Saudi Arabia accelerates industrial digitalisation.

With OT–IT convergence accelerating across energy, utilities, transport and manufacturing, what new vulnerabilities are you seeing, and how does Forescout help organisations secure these blended environments?
OT–IT convergence is expanding the attack surface dramatically. Many organisations are transitioning from legacy, isolated systems to highly connected environments with an increasing number of IoT and smart devices. This shift introduces vulnerabilities related to outdated platforms, misconfigurations, and devices that were never intended to be exposed. Forescout supports organisations by identifying every

CONTINUED ON PAGE 4

Seclore
Data Security Intelligence Framework

CONTINUED FROM PAGE 1

Data-centric...

maturity. Enterprises and government bodies have invested heavily in frameworks, technologies, and talent.

The biggest opportunities now lie in:

- advancing AI-driven security
- integrating identity and data governance
- strengthening automation within security operations
- addressing gaps introduced by cloud expansion and decentralised data flows

AI, in particular, is a major enabler. New innovations introduce fresh challenges and require security architectures capable of scaling with these emerging risks. Saudi organisations are ambitious and forward-thinking, and we see the Kingdom playing a leadership role in defining the future of secure digital transformation.

How does Seclore's product strategy align with Saudi Arabia's national visions and ongoing digital transformation initiatives?

Saudi Arabia's digital ambitions — from giga-projects to AI-native smart zones — require new approaches to protecting data in motion and at rest.

Seclore aligns directly with these national priorities by delivering continuous visibility, intelligence, and control over data as it moves across increasingly complex ecosystems. Whether organisations are adopting sovereign cloud, scaling AI, or modernising infrastructure, Seclore provides the security backbone that supports innovation without compromising compliance or sovereignty. The Kingdom's leadership in regulation and its bold digital roadmap make it an ideal environment for Seclore's platform.

What strategic value does Seclore gain by participating in Black Hat MEA 2025, and how does it support your engagement with regional stakeholders?

Black Hat MEA offers a unique opportunity to meet customers, regulators, and industry leaders who are driving cybersecurity transformation in the region.

For Seclore, it is a platform to:

- demonstrate the relevance of our technologies
- deepen engagement with strategic customers
- collaborate with local partners
- understand emerging sector-specific challenges
- contribute to national cybersecurity dialogue

Participation helps us stay close to the regional ecosystem and ensure our roadmap continues to align with the ambitions of the Kingdom and wider Middle East.

CONTINUED FROM PAGE 1

Forescout...

device—managed or unmanaged—profiling its behaviour, and applying automated policy-based controls. This helps maintain security as industrial networks evolve and adopt modern technologies.

Gaining real-time visibility into OT assets remains a major challenge in the Middle East. How does Forescout's platform address unmanaged devices, legacy systems and segmentation gaps across industrial networks?

Unmanaged and legacy devices continue to be one of the biggest risks in IT and OT environments. Forescout provides deep, continuous visibility into all assets the moment they appear on the network, without requiring agents. We detect devices across previously siloed segments, highlight gaps in network segmentation, and allow operators to enforce micro-segmentation with precision. This enables organisations to secure legacy infrastructure while progressively modernising their industrial architecture.

As Saudi Arabia scales giga-projects and smart city deployments, how is Forescout supporting critical infrastructure operators in building secure-by-design OT ecosystems?

Saudi Arabia's giga-projects and smart city initiatives depend on highly interconnected OT–IT environments. Forescout helps operators design networks where security is embedded from the start, not added later. Modern smart facilities no longer rely on a single, flat network; they have multiple specialised systems that must be isolated, monitored, and managed intelligently. Our platform provides the orchestration layer that enforces segmentation, monitors device interactions, and ensures that every asset maintains compliant behaviour across expanding digital infrastructures.

Ransomware groups and nation-state actors are increasingly targeting OT environments. What does Forescout's threat intelligence indicate about evolving attacker behaviour in the region, and what defensive actions should organisations prioritise?

Threat actors are becoming more sophisticated, and they are actively exploiting the complexity of modern industrial environments. Ransomware groups and nation-state adversaries are leveraging unmanaged devices, legacy assets, and segmentation blind spots to move laterally and disrupt operations. Forescout's threat intelligence provides continuous visibility into these behaviours, allowing organisations to detect anomalies early and respond before attackers can achieve impact. The priority now is to adopt automated detection, enforce segmentation, and maintain continuous monitoring across every device and protocol used in OT ecosystems.

Nozomi Networks showcases AI-powered OT/IoT security innovations

Nozomi Networks, the leader in OT,IoT security, today, announced its participation at Black Hat MEA 2025, taking place from December 2-4 at RECC Malham, Saudi Arabia. The company will showcase Guardian Air, the wireless sensor for visibility and security for OT and IoT environments and Nozomi Arc, its host-based security sensor that detects and defends against malicious or compromised endpoints.

At the event, Nozomi Networks will demonstrate its advanced monitoring, AI-driven analytics, and risk management tools designed to support critical infrastructure cyber resilience especially in industries including energy, utilities and transportation. It will also highlight the importance of securing converged OT/IoT environments with AI-driven visibility and threat detection through its comprehensive platform including Guardian, Vantage, Arc, and Guardian Air components.

Saudi Arabia has retained its global leadership in cybersecurity for 2025, according to the IMD World Competitiveness Yearbook, highlighting the nation's commitment to securing its digital and industrial ecosystems. This commitment is reflected in the National Cybersecurity Authority's Operational Technology Cybersecurity Controls (OTCC-1:2022), a regulatory framework to strengthen the cybersecurity posture of industrial and critical infrastructure systems across organisations operating critical national infrastructure.

Speaking on its participation, Muath Alsuwailem, Regional Sales Director, Nozomi Networks said, "With Saudi Arabia making significant strides in cybersecurity, Black Hat MEA provides an ideal platform to raise awareness around OT cybersecurity in critical industries as safeguarding operational technology and IoT environments is essential for both national security and business continuity. Our participation enables us to engage directly with regional decision-makers and showcase how leading organisations are securing resilience, visibility, and compliance across their cyber-physical systems using our AI-driven solutions. Our goal is to strengthen relationships with existing clients and partners in the region while introducing our latest innovations to new audiences."

In line with the Kingdom's cybersecurity initiatives, Nozomi Networks supports cyber resilience by enabling compliance with OTCC and leading global standards such as ISA/IEC 62443 and the NIST Cybersecurity Framework, while delivering integrated IT/OT visibility and automated risk management to address the challenges of an expanding attack surface. The Nozomi Networks platform addresses the full OT/ICS cybersecurity lifecycle with capabilities that align with the NCA mandate.

Nozomi Networks was recently recognised as the only vendor in the Gartner® Peer Insights™ Customers' Choice for CPS Protection Platforms and was also named a Leader in IoT Security Solutions by Forrester.

Attendees can visit the company at stand number H1.T80 and gain insights on how organisations are confidently addressing IEC 62443 and other compliance frameworks and get a firsthand experience of Nozomi Networks' solutions in action.

CPI Corporate Publishing International Ltd. tahawultech.com

cnme computer news middle east | Security Advisor Middle East | Reseller Middle East | 60 MINS LIVE عربية | GovTech

Founder, CPIMEDIA GROUP **Dominic De Sousa** (1959-2015), Group Publishing Director **Kausar Syed**, Sales Director **Sabita Miranda**,
Editors **Mark Forker, Sandhya D'Mello, Daniel Shepherd**, Designer **Prajith Payyapilly**, Web Developer **Adarsh Snehajan**

Quantum reality check: Race to secure data has already begun, says CTO Janne Hirvimies

QuantumGate's Janne Hirvimies warns that harvested data is already at risk — and organisations must accelerate their post-quantum readiness now.

Quantum computing is rapidly reshaping the security assumptions that have guided digital infrastructure for decades. The shift to post-quantum cryptography is no longer a distant milestone on global roadmaps; it has become an urgent, multi-year undertaking that many organisations still underestimate.

QuantumGate CTO Janne Hirvimies spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, about the industry's readiness and emphasised that the threat has already started, driven by "Harvest Now, Decrypt Later" tactics where adversaries quietly intercept encrypted data today with the intention of unlocking it once quantum capabilities mature.

Hirvimies highlights the UAE's early national stance on quantum resilience, while underscoring the sheer complexity of replacing cryptographic foundations embedded across applications, devices, protocols, and critical infrastructure. For leaders, he argues, the challenge is not only technical but cultural — requiring crypto agility, long-term planning, and collaboration across hardware ecosystems, cloud platforms, regulators, and service operators.

You've often spoken about the illusion of time in cybersecurity transformation. Why do you believe the timelines many organisations set for quantum migration are dangerously optimistic?

Many organisations take comfort in dates like 2030 or 2035 that appear in global post-quantum roadmaps. The set timelines often create the impression that there is still room to wait and that the risk is far away. The threat, however, does not begin when quantum computers become fully capable. It begins the moment attackers start harvesting encrypted data with the intention of decrypting it in the future. That is already happening today, which means time is not on our side.

Another misconception is how long migration takes. Moving to post-quantum cryptography is a multi-year transformation that affects applications, devices, protocols, and long-lived data. Even the first step, which is identifying where cryptography is used across an environment, can take six to eight months in a large organisation. During crypto discovery, we often uncover what teams describe as "shadow cryptography" — keys, certificates, and embedded mechanisms organisations did not know existed. This hidden complexity is what turns long timelines into urgent ones.

The UAE recognised this early and through the UAE Cybersecurity Council (CSC) the country set a clear path for quantum readiness and highlighted the importance of sovereign, in-country cryptographic capabilities. Protecting long-lasting national data depends on keeping algorithms, libraries, and key management under national oversight and aligned with the country's cybersecurity strategy. The real illusion of time is not only the calendar date. It is the assumption that change can happen quickly.

Many organisations still treat post-quantum readiness as a future concern. How would you convince leaders that the "Harvest Now, Decrypt Later" threat is already real and needs immediate attention?

The most effective way to show leaders that this threat is real is to focus on the data itself. Encrypted information that needs long-term protection is already exposed. Government records, healthcare files, financial histories, intellectual property and research data often require confidentiality that lasts for many years. Once any of this information is intercepted and stored by an adversary, it remains vulnerable until quantum computers can break the public key algorithms that protect it, such as RSA and ECC.

Data stays vulnerable for as long as it relies on today's public key encryption standards. If confidential information is being shared or transmitted, there is a real risk it can be harvested. Once this happens, control over that data is lost, and an adversary can simply wait until quantum computers allow them to decrypt it.

This is the reality behind Harvest Now Decrypt Later. Attackers do not need quantum computers today; they only need access to the data, for instance, while it is moving across networks or through compromised infrastructure. The moment it is collected, the exposure begins.

From your two decades in hardware-based mobile security, how do you see the evolution of cryptographic systems that are now deeply embedded across devices — and why does that make migration so complex?

For nearly fifty years, the cryptography we rely on has remained stable. The same public key foundations became the basis for authentication, secure access, and digital transactions. Updates happened over time, such as increasing key lengths or retiring from individual algorithms, but they were gradual. The overall trust model remained unchanged.

Because of this long period of stability, public key cryptography is built into every layer of modern infrastructure and into the mechanisms that secure how systems operate. It underpins how devices exchange data, how certificates function, and how digital trust is established across mobile, cloud, IoT and industrial environments. This model has served as the bedrock of security for decades.

The challenge now is that the entire foundation of public key cryptography needs to change. Post-quantum algorithms introduce new ways of establishing keys and creating signatures, and this affects every system that relies on the existing PKI model. Since the same approach has been adopted everywhere for forty years, the migration is complex. We are updating the base layer that everything else depends on.

What are the biggest misconceptions enterprises hold about the speed at which they can transition to quantum-safe systems?

One major misconception is the idea that moving to quantum-safe systems is like a routine software update. The change goes much deeper. It affects software libraries, communication protocols, embedded code, and often the hard-coded algorithms inside legacy hardware. Many of these components were never designed for rapid replacement.

Another misconception is the belief that organisations can wait for mandates or off-the-shelf solutions before acting. When everyone begins at the same time, pressure builds across the entire ecosystem. Suppliers become overwhelmed, costs rise, and there is little space for careful testing or phased rollout. Starting early is what prevents that bottleneck.

There is also the assumption that migration fits into a short project window. In practice, this work spans years. Before any upgrade can happen, organisations need a full picture of where cryptography sits across their environment, which can take many months. Only then can they prioritise, test, integrate, and gradually cut over to new quantum safe mechanisms. Fault-tolerant quantum computers are still in development, but progress is accelerating, and the timelines are tightening.

QuantumGate positions itself at the frontier of secure communication and applied cryptography. What role do secure hardware platforms and key-management innovation play in accelerating quantum migration?

Secure hardware and key management are both important in quantum safe migration, but neither is a one-size-fits-all approach. Each addresses different parts of the problem. Hardware anchored keys provide strong assurance for high value assets, yet they also come with cost, operational complexity and long replacement cycles. If a migration depends only on hardware, these factors can slow progress across the wider environment.

This is where key-management innovation becomes essential. Post-quantum migration increases the number and types of keys organisations must handle, and in many cases quantum-safe keys can be deployed directly to devices like mobile phones, providing strong security without the expense of dedicated hardware.

Sovereign capability also matters for leaders responsible for national or critical infrastructure. In the UAE, the Technology Innovation Institute's (TII) cryptographic libraries provide an in-country, certified foundation that integrates with both secure hardware platforms and large-scale key management systems. This gives organisations a clear path that matches national requirements.

In practice, secure hardware and modern key management work best together. The right combination supports quantum safe adoption in a way that is practical, secure, and aligned with the realities of each environment.

You've led security architecture development across global chipset and mobile ecosystems. How can industry-wide collaboration shorten the pilot-to-production cycle for quantum-resistant solutions?

Industry-wide collaboration is not just helpful for quantum migration, but essential. Cryptographic systems only work when they are interoperable, meaning devices, platforms, certificate authorities, and communication protocols must support the new algorithms in a consistent way. If one layer lags, the entire chain slows.

Standards bodies such as NIST and ETSI define the algorithms, but real progress happens when hardware makers, cloud providers, software developers, regulators and service operators test and validate these changes together. Shared pilots reveal performance characteristics, integration issues, and interoperability gaps early, which prevents

CONTINUED ON PAGE 6

> **Moving to post-quantum cryptography is a multi-year transformation that affects applications, devices, protocols, and long-lived data.**

Black Hat MEA becomes world's largest cyber security gathering, increasing in size by 55%

Black Hat MEA opened on Tuesday with a surge of energy as global CISOs, founders, policymakers and researchers gathered in Riyadh to decode the next wave of cyber risk. Day one delivered high-pressure intelligence, frontline lessons and live research across the Executive Summit, Briefings, Deep Dive and Campus stages.

This year's Black Hat MEA marks a 55% increase in size from last year, reinforcing Saudi Arabia's position as a hub for cybersecurity innovation and commercial growth.

Black Hat MEA began with the Opening Ceremony, followed by opening remarks from Eng. Muteb Alqany, CEO, Saudi Federation for Cybersecurity, Programming and Drones.

Alqany said, "With attendees from more than 163 countries, 500 global brands, and 300 speakers, Riyadh has become the meeting point for the global cybersecurity industry. Our shared goal is clear: to make the digital world safer, smarter, and stronger. Behind the scale is real impact – from turning regional startups into global competitors to delivering world-class training with a 92% approval rating. Together, we are shaping the future of cyberspace."

From the first moments of Black Hat MEA, one thing was clear: Riyadh has become the cyber world's preferred control room. Day one moved fast, with conversations that felt less like panels and more like intelligence exchanges between people who defend real targets under increasing pressure.

Faisal Al-Khamisi, Chairman of SAFCSP and Co-Chairman of Tahaluf, said "Black Hat MEA reflects the Kingdom's commitment to developing an advanced cybersecurity ecosystem built on specialised knowledge and national expertise. Through our partnerships with local and international entities, we work to empower national solutions to compete according to global standards."

Steve Durning, Portfolio Director of Black Hat MEA at Tahaluf, commented "What happened across the stages today is exactly why the world comes to Riyadh. We saw CISOs, founders, policymakers and researchers challenging each other and breaking down the hard problems. This is how resilience is built. Day one set the tone for a week where ideas become action and collaboration becomes capability."

Across the venue, Briefings and Deep Dive sessions revealed new vulnerabilities, research breakthroughs and exploit logic from global experts. Black Hat Campus drew rising talent with a keynote from 17-year-old cybersecurity specialist Bandana Kaur, while the Activity Zone's SAR 1 million prize fund, alongside Arsenal Labs, the Terminal and the Root Lounge, kept attendees hands-on with real systems under real pressure.

Annabelle Mander, Executive Vice President at Tahaluf said, "The energy across day one showed how far the Kingdom has come in building a world class cybersecurity industry. Riyadh is now one of the places where the future of government and enterprise security is being written."

One of the early standout moments came from Devon Bryan, global chief security officer at Booking Holdings, who broke down what it now takes to truly know a network and expose its weak points before adversaries do.

Later, Ricardo Lafosse, Gary Hayslip, Dr Chenxi Wang, Lance James and Jaya Baloo took the stage to chart the cyber shift from 2020 to 2025. Their discussion cut through theory and focused on the operational reality of today's threat landscape, where speed, AI tooling and attacker creativity are rewriting defensive playbooks in real time.

The day's tempo escalated with Jennifer Ewbank and Rich Baich, who walked the audience through the CIA's digital transformation and the lessons learned from defending a target that adversaries probe around the clock. Their fireside session was one of the most anticipated of the day, offering rare insight into resilience at an intelligence-agency level.

In the afternoon, the discussion widened with a sharp exchange led by Bjorn Watne of INTERPOL and Abdullah AlQahtani of the Ministry of Investment, who unpacked the economics of threat and where nations should focus resources next. The conversation made clear that national strategies must evolve as fast as attacker capabilities.

Cisco's Splunk cloud platform: Accelerating digital resilience for Agentic AI era in Saudi Arabia with Google Cloud

- Beginning 3 December, Splunk Cloud Platform on Google Cloud is available to Saudi organisations through in-country data centres.
- Businesses in The Kingdom can now harness the potential of their data in a secure, scalable, localised cloud environment, with an experience optimised for Google Cloud
- Availability of this platform reinforces Splunk's commitment to the region, and supports enhanced cybersecurity, a key pillar of Vision 2030

Cisco, the worldwide leader in networking and security, announced today the availability of Splunk Cloud Platform, its fully-managed data platform, on Google Cloud in the Kingdom of Saudi Arabia. The announcement, made during Black Hat MEA 2025, one of the major cybersecurity conferences taking place in Riyadh, marks an important milestone in expanding Splunk's regional footprint and supports Saudi Arabia's Vision 2030 goals, aiming to strengthen cybersecurity, cloud adoption and advance digital transformation.

Strengthening security and cloud resilience

The Splunk Cloud Platform brings observability and security together with end-to-end visibility, AI-driven detections, and automated response for greater digital resilience. As a unified data and AI platform, Splunk Cloud ensures that an organisation's data strategy drives its AI strategy. This enables organisations to unify data at scale, simplify operations with AI-first experiences, and transform machine data into AI-ready intelligence. This fuels cross-domain insights, operational excellence, and transformative innovation across the organisation.

With the Splunk Cloud Platform hosted in Google Cloud's in-country data centres – from 3rd December – organisations in Saudi Arabia stand to benefit from enhanced visibility and connectivity across their digital systems. By unifying observability and security, Splunk Cloud Platform enables faster issue detection and resolution through richer context and sharper analysis, empowering teams to act before issues affect operations or security. Organisations

can optimise their data lifecycle with full control over data structure, filtering, and routing to meet business and compliance needs. The platform also supports prompt onboarding, efficient management, and local data storage in line with residency requirements, and enhanced security as business needs evolve.

Delivering an optimised local cloud experience

Splunk Cloud Platform, running natively on Google Cloud Platform, will offer the latest Victoria experience – an architecture that offers enhanced admin capabilities and scalability. This will allow for Streamlined onboarding onto Google Cloud, simple management of both Splunk and Google Cloud services, and aims to offer the scalability organisations need as they grow.

Splunk will offer core solutions including Splunk Enterprise Security for real-time threat detection, investigation, and response, and Splunk IT Service Intelligence for comprehensive observability and performance monitoring, with the aim to help businesses enhance their operational resilience and facilitate innovation.

Mamduh Allam Area Vice President KSA, Bahrain & Kuwait at Splunk, said: "This launch represents a strategic leap forward for Saudi Arabian enterprises, with the intention to provide them with the tools to harness the potential of their data in a secure, scalable, and localised cloud environment. By bringing its next-generation platform to Google Cloud in Saudi Arabia, Splunk is directly addressing the growing demand for advanced digital resilience solutions, critical for the nation's ambitious Vision 2030 initiatives."

"We are thrilled to expand our partnership with Cisco to deliver the Splunk Cloud Platform natively on Google Cloud in the Kingdom of Saudi Arabia. By combining Splunk's unified security and observability capabilities with Google Cloud's secure, scalable, and AI-ready infrastructure, we're directly enabling Saudi enterprises to accelerate their journey towards Vision 2030," said Bader Almadi, Country Manager, Kingdom of Saudi Arabia at Google Cloud. "Our in-country data centers provide the trusted, local foundation that enables Saudi organisations to meet local data residency requirements while unlocking new opportunities for deeper, cross-domain insights and true digital resilience."

CONTINUED FROM PAGE 4

Quantum...

costly rework later. Collaboration does more than shorten timelines. It makes the transition possible.

Beyond technology, what cultural or organisational inertia prevents decision-makers from acting faster on quantum resilience — and how can this mindset be shifted?

Many decision-makers still assume they have time or believe the threat is too distant to compete with more immediate priorities. This creates a kind of scope blindness. When leaders underestimate how deeply cryptography is woven into their infrastructure, they plan a small fix instead of recognising the scale of the modernisation required.

Another challenge is the perception that cryptography is stable and slow-moving. That was true for decades, but the field is evolving quickly. Algorithms, standards, and best practices are shifting faster than before, which means organisations need crypto agility, the ability to adopt new algorithms and key-management approaches as they emerge. Post-quantum migration should be viewed not only as a security requirement but also as an

Anomali to showcase vision for AI-powered threat intelligence

Samer Jadallah, Vice President, Sales – Middle East and Africa, Anomali, spoke to Tahawultech.com about how AI-native threat intelligence, unified analytics, and cloud-ready architectures are transforming cyber defence in Saudi Arabia and beyond.

Black Hat MEA 2025 arrives at a pivotal moment for the region's cybersecurity landscape, where AI-driven threats, hybrid-cloud expansion, and large-scale national digital programmes are reshaping security priorities across Saudi Arabia. Organisations are demanding deeper visibility, faster response capabilities, and intelligence-driven operations that can keep pace with both the scale and sophistication of modern adversaries.

Anomali is preparing to showcase its vision for the future of threat intelligence—one built on agentic AI, unified analytics, and cloud-native security architectures designed for the Kingdom's rapidly evolving digital infrastructure. The company's leadership sees Saudi Arabia not only as a major hub for innovation but as a global benchmark for how nations can build cyber resilience at scale.

During a conversation with Tahawultech.com, Samer Jadallah, Vice President - Middle East and Africa, Anomali, shared insights into how Anomali is enabling faster decision-making, proactive threat hunting, and seamless visibility across complex environments. Jadallah also reflected on Black Hat MEA's transformation into a global cybersecurity powerhouse and what the industry can expect from the 2025 edition.

What is your perspective on Black Hat MEA's evolution and what do you expect from the 2025 edition?

I've attended Black Hat MEA from the very first edition, and it exceeded global expectations from day one. Every year, it becomes bigger, more sophisticated, and more influential. Last year's event surprised the global industry—not just in scale, but in the quality of insights and the depth of discussions. Today, Black Hat MEA is no longer a regional event. It attracts audiences from the US, Europe, and Asia—everyone wants to understand what Saudi Arabia is doing and how they can be part of this success story. I expect 2025 to bring even more surprises, strategic topics, and global participation.

How can Anomali help organisations maximise their existing security resources and reduce investigation and remediation times?

At Anomali, everything we do centres on shortening the time to detect and the time to respond. Our platform gives organisations deep visibility across their entire environment and allows them to instantly understand whether they are under attack, exposed, or safe. Unlike legacy technologies that offer a limited search window—often 60 or 90 days—we provide access to years of historical security data within seconds. This eliminates panic during incidents. Even small teams can operate at the scale of much larger SOCs because our platform automates correlation, analysis, and prioritisation. With this level of visibility and automation, organisations can confidently trust every critical alert and act much faster.

How can organisations shift from reactive detection to proactive threat hunting with real-time threat intelligence?

Proactive defence requires speed. When an attack happens anywhere in the world—whether in aviation, oil and gas, or government—security teams need actionable intelligence in real time. Anomali integrates intelligence from more than 150 trusted global feeds, removes false positives and irrelevant noise, and presents only high-fidelity alerts that matter to the organisation. Our threat-hunting workflow is powered by agentic AI combined with human expertise. We always say: "It's not AI versus AI; it's AI plus the human." This combination allows organisations to identify whether a global threat is relevant to them, determine exposure instantly, and act before attackers gain a foothold.

Customers can choose fully cloud, hybrid, or on-prem—whatever meets their regulatory obligations.

With AI accelerating both attacks and defences, how is Anomali using AI to improve correlation, attribution, and analyst decision-making?

AI has completely changed the rules of the game, both for attackers and defenders. A traditional investigation into a major global cyberattack could take days or weeks—and often happens during weekends or critical business hours. With Anomali, that entire process is reduced to under 15 seconds. Our AI engine analyses the attacker's TTPs, behaviours, and DNA of the attack, and compares it with up to 10–15 years of security telemetry. We support more than 25 languages, including Arabic, so analysts can simply ask questions in natural language:

"Am I exposed to this threat?" or "Show me the steps to protect my environment." This transforms decision-making and removes the need for complex queries or specialist skills.

As workloads move to the cloud, how is Anomali's cloud-native platform enabling unified visibility across hybrid and multi-cloud environments?

Cloud adoption is accelerating everywhere—and Saudi Arabia is no exception. Anomali was built cloud-native from day one on AWS, giving customers high availability, lower operational cost, and real-time updates.

For the Middle East, we have aligned closely with local cloud strategies.

- We launched support for AWS UAE cloud during GITEX.
- For Saudi Arabia, we are fully aligned with AWS Saudi, which will go live locally in 2026.
- For highly restricted environments such as defence, we offer a fully air-gapped deployment.

"Customers can choose fully cloud, hybrid, or on-prem—whatever meets their regulatory obligations. Our flexibility ensures every organisation can secure distributed environments without compromising data residency."

During large-scale events like Black Hat MEA, SOC teams face high alert volumes. What threat-intelligence capabilities are critical to maintain visibility and reduce false positives?

This is where our AI engine, Macula, becomes crucial. SOC teams are often flooded with alerts during peak periods, making it impossible to manually inspect everything. Macula sits at the core of our threat intelligence engine, collecting feeds from 150+ sources, eliminating false positives, deduplicating data, and surfacing only what is relevant. Instead of searching for "one grain of rice in a 10-kg sack," analysts receive a clean, prioritised, high-quality set of alerts. Nothing is missed, and analysts no longer rely on random sampling, which is the unfortunate reality in overloaded SOC environments.

How does Anomali's unified threat-intelligence platform consolidate detection, investigation, and response for multi-vector cyberattacks?

Most organisations use fragmented solutions—TIPs, SIEMs, SOARs, AI tools, each working in silos. Anomali unifies all of these capabilities into one security analytics platform. We ingest global threat intelligence, correlate it with the customer's environment using AI and natural-language processing, and then provide detection, investigation, and response capabilities from a single interface. There's no switching between tools or disconnected workflows. It becomes the organisation's single "moment of truth" for its entire security posture.

What indicators and intelligence signals does Anomali provide to help organisations quickly determine whether they are currently under attack?

Our platform delivers precise, high-confidence signals such as:

- Emerging risks relevant to the customer's industry
- Early indicators of compromise
- Behavioural patterns associated with known threat actors
- Exposure to new global breaches
- Validation of whether an active campaign affects the organisation

We help close the gaps between technologies and between teams—CTI, SOC, incident response, and business leaders. Instead of each working in isolation, Anomali ensures everyone shares the same intelligence and can act in a coordinated manner.

How is Anomali supporting Saudi Arabia's cybersecurity vision and strengthening national resilience against AI-driven threats?

Saudi Arabia is now one of the most strategically important cybersecurity markets in the world. Its digital transformation is extraordinary—and rapid digitalisation always attracts attackers. We work very closely with government entities, regulators, and decision-makers to support Vision 2030's cybersecurity priorities.

Our approach focuses on:

- Empowering organisations with AI-driven threat hunting
- Providing cloud-ready solutions aligned with local data residency requirements
- Strengthening national cyber resilience through real-time visibility
- Helping teams do "10× more" with the same resources, given the global cybersecurity talent shortage

We have a local office and a growing team in Riyadh because we believe deeply in the Kingdom's vision and want to support it long-term.

Group-IB charts next frontier of cyber defence in Saudi Arabia

Dmitry Volkov highlights how AI-driven threats, predictive security, and real-time fraud intelligence sharing are reshaping the Kingdom's cybersecurity ecosystem.

Saudi Arabia's cybersecurity landscape is entering a defining phase, shaped by rapid digital growth, AI-enabled threats, and a nationwide push for stronger cyber resilience. Against this backdrop, Group-IB is deepening its presence in the Kingdom, bringing adversary-centric intelligence, predictive defence capabilities, and new ecosystem-wide fraud prevention technologies to the market.

Dmitry Volkov, CEO of Group-IB, spoke to Daniel Sheperd, Online Editor, Tahawultech.com about how AI-driven cybercrime is reshaping risk, why collaborative defence models are becoming essential, and how the company's newly launched Cyber Fraud Intelligence Platform (CFIP) is set to transform real-time fraud intelligence sharing across Saudi organisations.

You've been expanding quickly in Saudi Arabia this year. What's driving demand for Group-IB's solutions across Saudi enterprises?

Saudi Arabia is a highly mature market, and organisations here know exactly what they want. They are looking for best-in-class technical capabilities that allow them not only to close gaps but to build advanced, service-driven security programmes. Demand for Group-IB stems from our adversary-centric approach and our ability to help enterprises focus on threat factors rather than just raw attacks. Because we conduct deep research on cybercriminal activity across global regions, our technologies allow customers to predict what may happen next and build stronger, more proactive cyber defences.

Looking at 2025 and beyond, what advanced Tactics, Techniques, and Procedures (TTPs) or threat groups are most actively targeting the Kingdom?

It varies by industry, but the overarching trend is clear: AI-enabled cybercrime is becoming the dominant threat. Fraud-focused criminal groups are adopting AI faster than any other segment—particularly video and voice deepfakes, which dramatically increase the success rate of scams. We also see sophisticated cyber attackers using AI to automate reconnaissance, vulnerability identification, and exploitation workflows. These AI-driven attacks operate at very high speed, so defenders need equally advanced technologies that can match or ideally anticipate the next step in the kill chain.

If you had to distil it into five points, what actionable threat insights should Saudi CISOs take away from Black Hat MEA 2025?

1. Shift away from legacy mindsets. Traditional security approaches no longer match the pace and sophistication of modern threats.
2. Adopt collective defence. Saudi enterprises need to collaborate more closely—sharing real-time cyber intelligence, fraud patterns, and threat telemetry.
3. Unify cyber and fraud operations. Criminals do not distinguish between these domains; defenders should not either.
4. Prioritise real-time intelligence. Rapid visibility into attacker behaviour is essential for resilience.
5. Move towards predictive security. AI-driven, behaviour-based modelling is the next frontier for advanced cybersecurity.

Tell us more about the CFIP launch. What technology sits behind it, and how does it solve gaps existing fraud systems cannot?

Every fraud system—behavioural, transactional, or rule-based—inevitably leaves gaps. Organisations increasingly want to share real-time fraud intelligence with banks, fintechs, telcos, regulators, and major e-commerce platforms.

The Cyber Fraud Intelligence Platform (CFIP) solves this by enabling live information exchange while ensuring zero sensitive data ever leaves the organisation.

Group-IB uses a patented tokenisation mechanism that allows entities to compare and correlate fraud signals without exposing personal or regulated data. This achieves two goals simultaneously:

- real-time collaboration across the ecosystem
- full compliance with privacy and data-protection requirements

This is a breakthrough because it bridges a long-standing gap between the need to share intelligence and the need to protect customer information.

How is Group-IB collaborating with Saudi companies and global vendors to build a more unified cybersecurity ecosystem?

We work closely with Saudi regulators, public-sector bodies, and major enterprises, helping strengthen national cyber resilience. Group-IB has built a full technical infrastructure and a local expert team within the Kingdom, ensuring our customers receive in-country expertise and support.

Our full-stack platform integrates across the technologies that organisations have already invested in—whether on-premises or cloud-based—so that existing tools are enhanced rather than replaced. This integrated approach helps automate routine actions, improve operational efficiency, and unify cyber and fraud defence across the ecosystem.

Etihad Salam and DTM collaborate, launching four advanced cybersecurity products

Etihad Salam Telecom Company (Salam), a leading provider of telecommunications services in Saudi Arabia, announces it has signed a partnership agreement with DTM, an expert in digital transformation and cybersecurity. Under the partnership agreement signed at Black Hat MEA 2025, they will be launching four advanced cybersecurity solutions designed to fortify digital protection for organisations across the Kingdom. As a trusted provider of cyber defense services, Salam continues to support public- and private-sector entities with seamless, secure operations as they contribute to building Saudi Arabia's digital infrastructure.

This collaboration comes at a time when cyber threats are increasing rapidly, with a 35% increase in reported cyberattacks in the Kingdom. These are showing greater sophistication, making enhanced visibility, faster response, and stronger security more critical than ever. This partnership with DTM demonstrates how Etihad Salam is expanding its defense portfolio with modern, high-impact solutions that empower enterprises to protect their systems, data, and users with confidence.

Commenting on the partnership, Abdullah Mohammad Khorami, Chief Business Officer at Salam, said, "DTM is a strategic partner in elevating the cybersecurity backbone our clients rely on. By integrating these advanced solutions, we are not just enhancing protection, we are shaping a more resilient digital ecosystem for Saudi Arabia. This step directly supports Vision 2030's drive for a secure, future-ready digital economy, and reinforces Salam's commitment to delivering stronger, smarter, and more adaptive defenses for organisations nationwide."

The newly launched products include Endpoint Detection and Response (EDR) for real-time monitoring and automated threat mitigation; Privileged Access Management (PAM) to safeguard high-risk accounts and minimise insider and credential-based vulnerabilities; an Anti-Fraud Solution that leverages behavioral analytics and real-time intelligence to detect and prevent fraudulent activity; and Secure DNS, which blocks malicious domains and phishing attempts, ensuring safe and reliable internet access.

Dmitry Samartsev, DTM Chairman, commented, "Our collaboration with Salam enables us to bring advanced, high-impact cybersecurity capabilities to organisations across Saudi Arabia. By combining our technical expertise with Salam's national reach, we deliver stronger, faster, and more adaptive protection."

The collaboration with DTM and Salam facilitates the delivery of cutting-edge cybersecurity capabilities that address the evolving risks faced by today's enterprises. It combines Salam's national reach with DTM's deep technical expertise to provide more secure, adaptive protection. Through partnerships such as this, Etihad Salam is helping build the digital architecture powering Saudi Arabia's digital future.

Fortify Your Cybersecurity
Fortinet
Global Cybersecurity Leader

OPSWAT to show mobile cybersecurity mini lab, media scanning kiosk

OPSWAT focuses on empowering organisations across key industries, including the finance, oil and gas, energy, defence, and government sectors, to stay ahead of evolving threats.

OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, will participate in Black Hat Middle East & Africa 2025 with demonstrations of its latest security innovations, including the OP/X Mobile Lab and MetaDefender Kiosk.

Marking its third consecutive appearance at the region's largest information security exhibition, OPSWAT will showcase how its cutting-edge technologies and integrated cybersecurity platform are transforming the defence of critical infrastructure amid an increasingly complex threat landscape.

OPSWAT will bring an immersive experience to Black Hat MEA, headlined by the debut of the OP/X Mobile Lab. This compact, interactive setup lets visitors explore how OPSWAT technology protects critical infrastructure across IT, OT, and cross-domain environments. The showcase will also feature the MetaDefender Kiosk, a robust hardware appliance that securely scans and sanitises removable media such as USB drives and SD cards. Leveraging over 30+ anti-malware engines and OPSWAT's industry-leading Deep Content Disarm and Reconstruction (CDR) technology, the Kiosk demonstrates real-time protection against one of the most persistent attack vectors in critical and air-gapped environments.

"As the region accelerates its digital transformation, organisations are placing greater focus on strengthening their cyber defences," said James Neilson, Senior Vice President, International at OPSWAT.

"At events like Black Hat MEA, we can demonstrate how our technologies enable government institutions and enterprises to stay ahead of threats by detecting, preventing, and responding to attacks before they can impact critical operations."

During the event, OPSWAT will also introduce Unit 515, its elite cybersecurity services division, specialising in adversarial simulation, vulnerability assessments, and threat emulation. By bringing the real-world perspective of seasoned cyber defenders, Unit 515 reinforces OPSWAT's mission to strengthen the protection of critical infrastructure and bridge the gap between IT and OT security practices.

Beyond technology, OPSWAT is championing the advancement of cybersecurity expertise through the OPSWAT Academy, which was recently recognised as a Continuing Professional Education (CPE) Partner for Cybersecurity by ISC2. During Black Hat MEA, OPSWAT will offer exclusive Academy vouchers for its Critical Infrastructure Protection Training, designed to equip professionals with the knowledge and certifications needed to secure IT, OT, and industrial control systems.

Amjad Quteifan, Regional Director, KSA at OPSWAT, noted that Saudi Arabia's swift digital expansion and strong commitment to cybersecurity are evident in the sector's contribution of nearly SAR 18.5 billion to the Kingdom's GDP in 2024. He added, "At OPSWAT, we see this progress as a call to action to strengthen our partnerships and accelerate technology enablement to support Saudi Arabia's objectives for a secure and self-reliant digital economy. At Black Hat MEA, we therefore showcase practical, scalable solutions designed to safeguard the region's critical infrastructure and enhance its cybersecurity ecosystem for the future."

OPSWAT focuses on empowering organisations across key industries, including the finance, oil and gas, energy, defence, and government sectors, to stay ahead of evolving threats. With AI-driven threat detection, multi-AV scanning delivering up to 99% malware detection rates, and zero-trust content disarmament, OPSWAT provides an integrated platform that helps enterprises reduce risk, prevent zero-day attacks, and achieve compliance in increasingly complex hybrid environments.

Visit the OPSWAT stand #R11 located in Hall 1 to see firsthand how the company is redefining critical infrastructure protection.

At events like Black Hat MEA, we can demonstrate how our technologies enable government institutions and enterprises to stay ahead of threats by detecting, preventing, and responding to attacks before they can impact critical operations.

StarLink to boost AI adoption, accelerate cyber defences and business growth

StarLink's comprehensive portfolio spans across five key areas - cyber resilience, cloud transformation, enterprise AI, agentic automation, and digital infrastructure.

StarLink, an Infinigate Group company, is once again showcasing advanced AI-powered cybersecurity solutions at Black Hat MEA 2025, Riyadh to accelerate AI adoption, strengthen cyber defences, and enable seamless business growth for organisations in the region.

Saudi Arabia is emerging as one of the world's most advanced AI markets, driven by substantial investments in AI infrastructure and cloud capabilities. According to recent studies, AI spending by organisations in KSA is growing at an impressive rate of 160% YoY. With major hyperscalers establishing state-of-the-art data centres in the Kingdom, a strong cloud foundation is rapidly taking shape - enabling and accelerating nationwide as well as regionwide AI adoption. This surge in AI adoption is not only driving innovation but also reshaping the risk landscape and data protection requirements, compelling organisations to deploy robust, AI-ready cybersecurity strategies.

Nidal Othman, CEO, StarLink, commented, "StarLink's presence at Black Hat MEA underscores our commitment to accelerating the Kingdom's AI agenda and supporting Saudi Arabia's Vision 2030 to become a global AI leader. With AI dominating today's conversations, we are ready to showcase how organisations can protect and harness AI-driven innovation securely.

"We are excited to play a role in shaping the region's AI-driven future and strengthening the journey toward enhanced cyber resilience."

StarLink's comprehensive portfolio spans across five key areas - cyber resilience, cloud transformation, enterprise AI, agentic automation, and digital infrastructure. Black Hat MEA where global expertise meet regional innovation, StarLink partners with key technologies - Beyond Trust, DigiCert, Endace, Exabeam, FireMon, F5, Forcepoint, Forescout, Fortra, IBM, Infoblox, Ivanti, LinkShadow, Okta, Palo Alto Networks, SecurX360, Sophos, Thales, Trend Micro and Yubico. Connect with the StarLink and vendor industry experts to experience the innovative array of solutions offering.

We are excited to play a role in shaping the region's AI-driven future and strengthening the journey toward enhanced cyber resilience.

رقميــات
Raqmiyat

Secure Your Digital Future

Simple. Secure. Resilient.

Secure Your Enterprise IT Footprint For A Safer Digital Journey

www.raqmiyat.com
UAE | KSA | INDIA

SentinelOne expands presence in Saudi Arabia with new Riyadh headquarters

The new headquarters will bring in-country expertise, direct partner support, and advanced cybersecurity skills training that aligns with Saudi Vision 2030.

SentinelOne, the leader in AI-native cybersecurity, announced the establishment of its new regional headquarters in Riyadh. The opening represents a major turning point in the company's expansion plan and ongoing dedication to the region. The new headquarters will be the main hub for SentinelOne's KSA operations and help support Saudi Vision 2030 for digital transformation, national cybersecurity, and modern government services. It also ensures that customers in the Kingdom have direct access to the knowledge required to protect their environments from evolving cyberthreats.

The headquarters, located in the Al Malqa district, welcomed SentinelOne staff members and key partners on December 1st. The new office will cater to all the requirements of clients and partners with customer success teams, local solution specialists, and partner enablement experts. The regional presence of these teams means a quicker response for support, including tailored services that meet local requirements.

“Saudi Arabia is one of the world's most dynamic and fast-growing digital economies, and our major investment in the new Riyadh headquarters reflects our confidence in the Kingdom's potential,” said Meriam ElOuazzani, Regional Senior Director, Middle East, Turkey and Africa, at SentinelOne.

“A focal point of our vision is to help develop local Saudi talent through training programs, hands-on workshops, and real-world learning. To provide future cybersecurity experts with useful pathways, we are establishing specialized threat-hunting labs and collaborating closely with academic institutions. These initiatives help the nation develop a highly qualified digital workforce and align with Saudi Vision 2030.”

The headquarters serves as a gateway for closer collaboration with Saudi partners, clients, and government organizations. SentinelOne's local operations enable it to support national cybersecurity initiatives more responsively, bolster resilience in crucial industries, and aid companies in achieving their digital transformation. The company's AI-native solutions will defend critical infrastructure, modern cloud environments, and dispersed endpoints and digital identities at scale by enabling autonomous threat detection, investigation, and response.

The Riyadh headquarters strengthens SentinelOne's reputation as a reliable partner for Saudi businesses looking to take proactive measures to prosper in an increasingly complicated threat environment. Continued investment in technology, talents and partnerships is essential as cyberattacks grow more complex. This commitment supports Saudi Arabia's digital transformation goals and gives local organizations the resources they need in a modern AI-powered business landscape.

> **Saudi Arabia is one of the world's most dynamic and fast-growing digital economies, and our major investment in the new Riyadh headquarters reflects our confidence in the Kingdom's potential.**
> ***Meriam ElOuazzani, Regional Senior Director, Middle East, Turkey and Africa, at SentinelOne***

Saudi Arabia's next leap in national cyber readiness and digital sovereignty

Saudi cybersecurity leaders highlight how AI governance, identity security, and OT resilience are becoming cornerstones of the Kingdom's secure digital economy.

Saudi Arabia is preparing to host one of the world's most influential cybersecurity events — Black Hat MEA 2025, a gathering that arrives at a defining moment for the Kingdom's digital transformation. While global attention often centres on cyber threats and technology trends, the Saudi narrative is broader and more strategic: building national cyber readiness, nurturing specialised talent, and safeguarding the digital foundations of a rapidly diversifying economy.

This year's edition of Black Hat MEA reflects the Kingdom's steady march toward digital sovereignty, where cybersecurity strategy is closely aligned with economic growth, industrial expansion, and technological innovation.

Workforce Built for Kingdom's Digital Future

Ned Baltagi, Managing Director, Middle East, Africa, and Turkey at SANS Institute, believes Saudi Arabia's strength lies in its structured investment in human capital. “Saudi Arabia continues to lead globally in cybersecurity, retaining its top position in the IMD World Competitiveness Yearbook 2025 cybersecurity indicator,” said Baltagi.

The Managing Director, Middle East, Africa, and Turkey at SANS Institute believes that workforce development is emerging as one of the Kingdom's most important long-term assets. “Our training aligns with the Saudi Cyber Security Workforce Framework (SCyWF), ensuring that learners gain skills mapped to nationally defined roles,” he explains.

Identity Becomes Front Line

The cybersecurity priorities of enterprises are shifting at the organisational level. Harish Chib, Vice President Emerging Markets, Middle East & Africa at Sophos, observes a clear direction: identity security is becoming the anchor of modern defence.

“Identity threat detection and response, MDR/XDR, and next-gen SIEM are moving to the centre of cyber readiness,” Chib says. With digital services multiplying across the country, security teams must ensure that access control, endpoint integrity, and incident response discipline remain strong—especially as ransomware operations grow more aggressive.

Autonomous Cyber Operations

For multinational and government entities operating at scale, the next cyber frontier is AI-driven automation. Ezzeldin Hussein, Regional Senior Director, Solution Engineering at SentinelOne, sees autonomous cybersecurity as a natural evolution of the Kingdom's digital ambition.

“AI-driven threats and defenses will now shape the region's security posture,” he states.

Attackers are using generative AI to create more convincing phishing, impersonation, and vulnerability exploitation. Hussein stresses that Saudi organisations must equip their SOC teams with AI-SIEM, hyperautomation, and agentic AI to reduce manual workloads and shorten response cycles.

Protecting Industry and National Infrastructure

While enterprise security advances rapidly, one of the most critical shifts is happening in industrial technology environments. Saudi Arabia's smart cities, energy facilities, manufacturing plants, and utilities are becoming highly interconnected—creating new exposures that must be managed with precision.

Mark Thurmond, Co-CEO, Tenable, said, “Saudi Arabia's digital transformation is rapidly expanding the Kingdom's attack surface, creating the need for unified visibility and AI-powered automation across IT, OT, cloud, and identity. Giga-projects like NEOM and the HUMAIN AI Zone are significantly accelerating the shift to cloud-driven and AI-native services, which in turn demand stronger governance aligned with the NCA Essential Cybersecurity Controls and PDPL.

CYBER READINESS BECOMES REALITY
WITH
COMMVAULT® CLOUD CLEANROOM™ RECOVERY
Commvault®
Visit commvault.com to Learn More