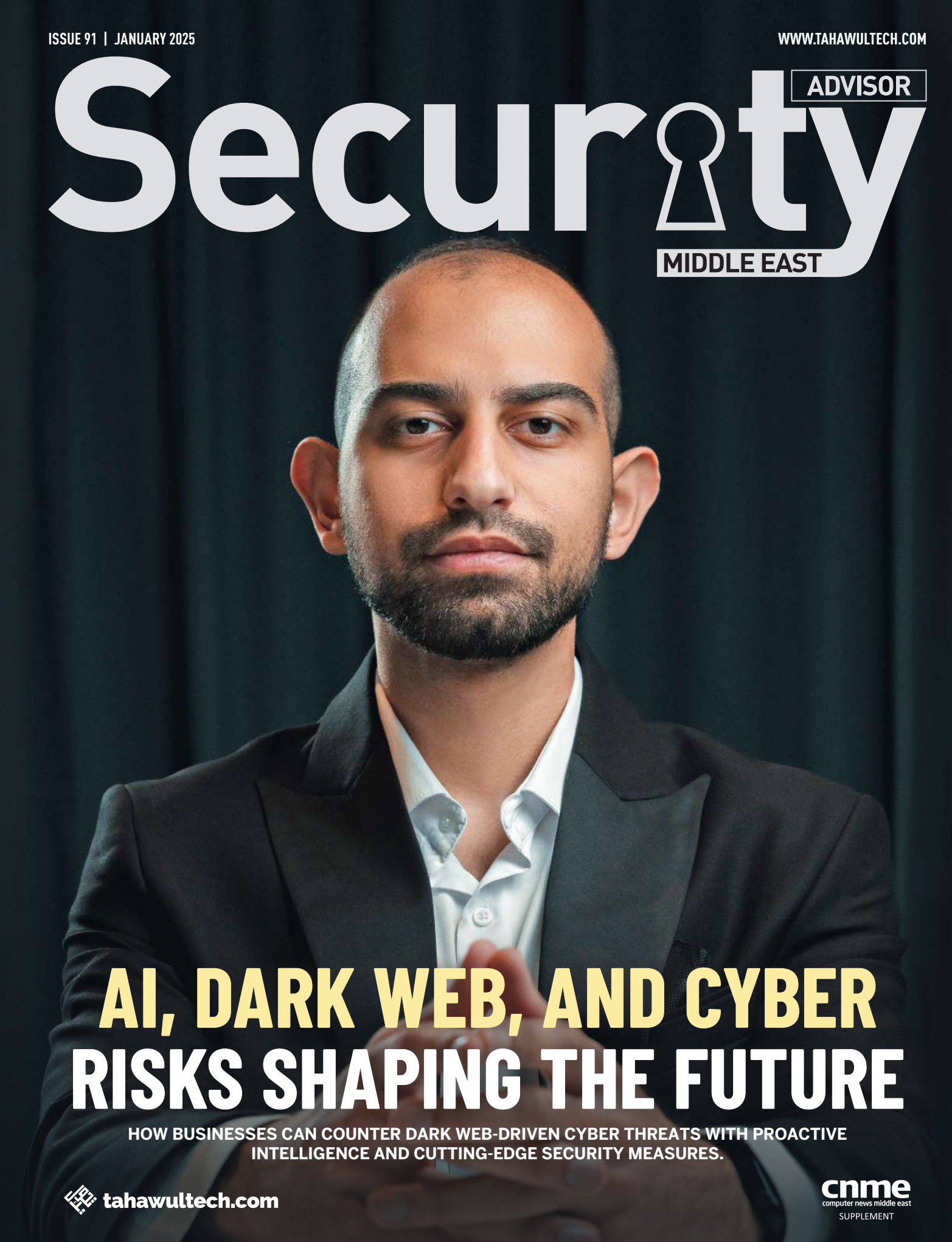
ISSUE 91 | JANUARY 2025

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST



AI, DARK WEB, AND CYBER RISKS SHAPING THE FUTURE

HOW BUSINESSES CAN COUNTER DARK WEB-DRIVEN CYBER THREATS WITH PROACTIVE INTELLIGENCE AND CUTTING-EDGE SECURITY MEASURES.

tahawultech.com

cnme computer news middle east SUPPLEMENT


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

CONTENTS

Security ADVISOR MIDDLE EAST

تحت الرعاية السامية لصاحب الجلالة الملك محمد السادس

Under the High Patronage of His Majesty King Mohammed VI

GITEX AFRICA Morocco

UNDER THE AUTHORITY OF | IN PARTNERSHIP WITH | ORGANISED BY

14 - 16 APRIL 2025 MARRAKECH

POWERING AFRICA INTO THE GLOBAL AI ECONOMY

AFRICA'S LARGEST TECH AND STARTUP EVENT JUST GOT BIGGER

45,000 ATTENDEES	**1,400** EXHIBITING & STARTUP COMPANIES
435 MEDIA ATTENDEES	**650+** GOVERNMENT REPRESENTATIVES
130+ COUNTRIES REPRESENTED	**340+** INVESTORS WITH $250 BILLION ASSETS UNDER MANAGEMENT
660+ SPEAKERS	**70%** OF INVESTORS PLAN TO INVEST IN STARTUPS

- Ai EVERYTHING MOROCCO (AI X CLOUD X IOT)
- DATA CENTRES NEW
- CYBERSECURITY
- TELECOM & NETWORK INFRASTRUCTURE
- DIGITAL CITIES
- E-MOBILITY NEW
- GITEX IMPACT (SUSTAINABILITY, CLIMATE TECH, AGRITECH) NEW
- HEALTHTECH 5.0
- FUTURE OF BANKING & FINANCE
- NORTH STAR AFRICA - STARTUPS

gitexafrica.com

/gitexafrica

SCAN TO GET INVOLVED

EDITOR'S NOTE

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

Sandhya DMello
Editor

STRENGTHENING CYBERSECURITY FOR A SAFER FUTURE

The cyber threat landscape is evolving rapidly, with AI-driven attacks, dark web threats, and ransomware posing new challenges for businesses. Organizations in the Middle East must stay ahead with proactive threat intelligence and robust defense strategies.

This issue of January 2025, Security Advisor Middle East explores critical developments shaping the cybersecurity ecosystem. Ahmad Halabi, Managing Director of Resecurity Inc., discusses dark web-driven cyber threats, AI's role in cybercrime, and the need for proactive security measures. Chainalysis' acquisition of Alterya strengthens fraud detection, while Cyble's recognition in Forrester's Q1 2025 report highlights its leadership in threat intelligence.

CYBER RESILIENCE – INSIGHTS, THREATS, STRATEGIES

DORA regulations continue to impact financial services, requiring stronger third-party risk management. Derek Manky of Fortinet emphasizes the need for industry-wide collaboration to disrupt cybercrime's financial model. Leadership shifts also mark the cybersecurity landscape, with Samer Abu-Ltaif taking the helm as Microsoft's President for EMEA and Shinichi 'Sam' Yoshida leading Canon EMEA.

Huawei's AI security advancements, Western Digital's innovations in AI-powered storage, and Genetec's security solutions at Intersec 2025 highlight the region's commitment to digital resilience. Meanwhile, Dubai-based Secure Domains introduces the region's first cloud-based DNS firewall, reinforcing cybersecurity capabilities in MENA.

The rise of Ransomware-as-a-Service (RaaS) groups, Cloudflare's call to eliminate vendor lock-in, and SANS Cyber Academies' workforce development efforts further underscore the importance of staying ahead in cybersecurity.

Security Advisor Middle East continues to bring timely insights, expert perspectives, and the latest security trends. The future of cybersecurity depends on readiness—now is the time to strengthen defenses.

EVENTS

tahawultech.com FUTURE SECURITY AWARDS

tahawultech.com CISO50 AWARDS & FORUM

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by CPI

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

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

PRODUCTION AND DESIGN
Designer
Prajith Payyapilly
prajith.payyapilly@cpimediagroup.com

DIGITAL SERVICES
Web Developer
Adarsh Snehajan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

CHAINALYSIS ACQUIRES ALTERYA, BOOSTS CYBERCRIME PREVENTION CAPABILITIES

Chainalysis has just announced its acquisition of Alterya, the AI-powered fraud detection solution that identifies scammers before they meet their victims. This deal follows the company's acquisition last month of the web3 security solution Hexagate, and represents the blockchain data leader's doubling down on its strategy to become the leader in the prevention and investigation of illicit transactions.

Jonathan Levin, Cofounder and CEO at Chainalysis said, "Our acquisition of Alterya represents a significant step forward in our work to provide a holistic risk solution that includes prevention, compliance and remediation. Their mission to protect humans everywhere from fraud and scams — one of the highest grossing categories of crypto crime annually — is integral to our mission to build trust in blockchains. We're thrilled to welcome Alterya to the team and to work on safeguarding billions of people from fraud and delivering safer and faster payments for all."

These major investments by Chainalysis come at a time when the continued mainstream adoption of cryptocurrencies is driving a pressing need for governments, law enforcement agencies and Virtual Asset Service Providers

(VASPs) to implement robust frameworks to detect crime and protect consumers. In 2024 alone, illicit addresses received a whopping US$40.9 billion — a figure that Chainalysis estimates will rise to US$51 billion as it continues to refine its analysis.

Alterya already works with top cryptocurrency exchanges and fintech companies including Binance, Coinbase, and Block, as well as top financial institutions, to monitor more than US$8 billion in transactions per month across crypto and fiat rails to protect 100 million end users from the growing threat of authorized fraud. Last year, the company detected US$10 billion sent to scams, and worked with their customers to proactively prevent fraud, minimize losses, and build customer trust.

With this acquisition, Chainalysis can now provide real-time proactive fraud protection for payments and enhanced fraud detection during KYC for exchanges, blockchains, and wallet providers. Government agencies may also leverage Alterya's insights for lead generation into pig butchering, scams, and other emerging authorized fraud trends. Chainalysis will continue to build upon Alterya's collection of fraud identifiers on fiat payment rails to provide insights to financial services firms on the fiat accounts where customers are losing money to fraud — often an early red flag before funds move into crypto.

Alterya customer, Ilan Zimmer, Director of Payment & Operational Risk at Coinbase, commented, "Alterya has been a reliable partner in helping Coinbase identify wallet addresses tied to known investment scams. This collaboration has enabled us to better protect our customers and safeguard their hard-earned funds from bad actors."

MECOMED LAUNCH DISTRIBUTORS' NETWORK TO ADVANCE MEDTECH INDUSTRY COLLABORATION IN MEA

Mecomed, a Medical Technology Association in the Middle East and Africa, announced the launch of its Distributors' Network, a initiative aimed to encourage collaboration among Mecomed associate members to address distributor-specific topics while contributing to developments in healthcare across the Middle East and Africa (MEA) region.

The event welcomed leaders and senior executives from MedTech distributor companies in the MEA region, including both Mecomed members and non-members, creating a dynamic platform for collaboration. It commenced with a non-competition law reminder to the attendees, emphasizing compliance with regulations and reinforcing Mecomed's dedication to upholding the highest ethical standards in its operations.

"The launch of the Distributor Network represents a pivotal moment for Mecomed, as it enables us collaboratively advance healthcare delivery standards across the MEA region." said Rami Rajab, CEO of Mecomed. "By promoting collaboration and transparency, we aim to drive impactful progress for both the industry and the patients we serve."

Attendees were also introduced to revised Mecomed's Code of Ethical Business Practices, which sets the standard for compliance and integrity within the MedTech industry, highlighting Mecomed's commitment to promoting transparency and operational efficiency.

This event reinforces Mecomed's commitment to being the voice of the MedTech industry in the region, driving collaboration and innovation to address key challenges and improve healthcare outcomes.

TENABLE PLANS TO ACQUIRE VULCAN CYBER, ACCELERATE LEADERSHIP IN EXPOSURE MANAGEMENT

Under the terms of the agreement, Tenable will acquire Vulcan Cyber for approximately $147 million in cash and $3 million of restricted stock units (RSUs) that vest over a future period.

Tenable Holdings, Inc., (Tenable) the exposure management company, today announced that it has signed a definitive agreement to acquire Vulcan Cyber Ltd. (Vulcan Cyber), a leading innovator in exposure management. Vulcan Cyber's capabilities will augment Tenable's industry-leading Exposure Management platform, enhancing customers' ability to consolidate exposures across their security stack, prioritize risks and streamline remediation efforts across the entire attack surface.

Under the terms of the agreement, Tenable will acquire Vulcan Cyber for approximately $147 million in cash and $3 million of restricted stock units (RSUs) that vest over a future period. The acquisition is expected to close in the first quarter of 2025, subject to customary closing conditions.

"CISOs are overwhelmed with scattered security products, siloed tools and disjointed teams which makes protecting their organizations from exposure a massive undertaking. As the pioneer behind Exposure Management, we are driven to solve this central challenge of modern security — a fragmented approach to identifying and combating cyber risk," said Steve Vintz, Co-CEO and CFO, Tenable.

"With Vulcan, we're accelerating our Tenable One vision to radically unify security visibility, insight and action across the attack surface – from the data center to the cloud – to rapidly expose and close the gaps that put businesses at risk."

Tenable plans to expand the Tenable One Exposure Management Platform with Vulcan Cyber's robust capabilities, including enhanced visibility, extended third-party data flows, superior risk prioritization, and optimized remediation. By consolidating and aggregating vast amounts of data into the most comprehensive Exposure Management platform, Tenable is empowering organizations to confidently reduce risk across their entire environment.

"These capabilities aren't just technical

enhancements – they represent a fundamental shift in how organizations will manage cyber risks holistically into the future. For example, while having a cloud security platform is critical on its own, its power is exponentially amplified when treated as part of a comprehensive exposure management approach," said Mark Thurmond, Co-CEO and COO, Tenable. "By uniting disparate tools and data under one roof, we're providing security teams with a full-spectrum view of their attack surface, enabling them to prioritize what matters most and act decisively to address vulnerabilities."

A Unified Vision for Exposure Management

With the addition of Vulcan Cyber, Tenable One customers will gain:

- Expanded Third-Party Ecosystem Data: By integrating with more than 100 security products across vulnerability assessment, endpoint security, cloud security, application security, and threat intelligence, Tenable will ingest, normalize, and unify data across the security stack. This streamlined approach centralizes critical data and empowers security teams to operate more efficiently and proactively across the entire attack surface.
- AI-Powered Risk Prioritization: Siloed security products create blind spots where attackers thrive, leaving critical gaps across the attack surface. Enhanced risk prioritization closes these gaps by integrating enriched threat intelligence and context, helping organizations focus on the most critical vulnerabilities while optimizing the use of their security tools and technology.
- Automated Remediation Workflows: Optimized remediation with automated campaigns, advanced tagging and ticketing ensure that security issues, along with corrective guidance, get into the hands of the right security team members to automatically fix exposures quickly, wherever they might exist in their environment.
- Advanced AI capabilities: Leveraging a single unified risk data set, Tenable is laying the foundation for advanced exposure AI capabilities that will revolutionize how customers manage and mitigate risk across the security stack.

"We're thrilled to join forces with Tenable. Integrating Vulcan Cyber's capabilities into the Tenable One platform will uniquely address all exposure management use cases across the entire attack surface," said Yaniv Bar-Dayan, Co-Founder and CEO, Vulcan Cyber. "For the first time at scale, security teams will be able to consolidate exposure findings from multiple sources into a single, actionable interface. We are excited to start working with Tenable and their customers to remediate exposure risk."

WESTCON-COMSTOR BOLSTERS MULTI-VENDOR CYBERSECURITY DEMOS WITH AWS INTEGRATIONS

Westcon-Comstor, a global technology provider and specialist distributor, recently announced a new service enabling partners to experience the combined power of multi-vendor cybersecurity solutions and native Amazon Web Services (AWS) services in a dynamic virtual demo environment.

The distributor has added AWS integrations to its 3D Lab, which it created in 2022 to allow partners across EMEA (Europe, Middle East and Africa) to assess and validate security solutions against specific use cases prior to purchase.

Demos of products from the likes of Check Point Software, CrowdStrike, Infoblox, Palo Alto Networks and Zscaler can now be experienced in a secure, customisable and configurable AWS environment.

Through integrations with AWS services, partners and their customers can witness the additional value that multi-vendor solutions can bring when deployed on AWS.

Created by Westcon-Comstor in response to changes in end-user buying behaviour, 3D Lab is free to use and accessible within 48 hours of request.

Since launch it has generated $200m in new business for EMEA-based partners, with 26 use cases experienced by around 4,000 users in 45 unique lab environments.

The addition of AWS integrations to 3D Lab marks the latest milestone in Westcon-Comstor's growing collaboration with the cloud giant.

Early last year the distributor launched its AWS Marketplace programme, which unlocks new growth opportunities for partners by providing a streamlined and simplified route to transacting on the platform, supported by advisory and enablement services.

Then in November Westcon-Comstor become an authorised AWS distributor for Europe, adding to an existing distribution agreement in Asia-Pacific (APAC).

The 3D Lab integration enables a seamless, holistic journey whereby a partner can validate a security solution in an AWS environment, purchase it from Westcon-Comstor via either a private AWS Marketplace listing or the traditional route and then sell to an end-user.

"3D Lab is all about enabling partners to try solutions, enhance their knowledge and become trusted advisors to their customers – ultimately shortening sales cycles by moving from demo to decision, fast", said Daniel Hurel, Senior Vice President, Westcon EMEA Cybersecurity & Next-Generation Solutions at Westcon-Comstor. "Bringing AWS services into the mix though these exciting new integrations is the perfect next step in the evolution of 3D Lab, creating exciting new possibilities for security-focused partners while allowing us to leverage our expertise in cloud and AWS."

ZENDATA CYBERSECURITY BECOMES CREST-CERTIFIED IN BAHRAIN, LAUNCHES COMPLIANCE PACKAGES FOR SMES

ZENDATA Cybersecurity is now officially CREST-certified in Bahrain, allowing the company to provide Managed Security Services (MSSP) in full compliance with national regulations. With new cybersecurity legislation under Bahrain's National Cyber Security Center (NCSC) set to mandate a cybersecurity baseline for SMEs, only CREST-certified MSSPs will be authorized to deliver these essential security services.

To support businesses in meeting these requirements, ZENDATA is introducing three tailored cybersecurity packages for SMEs in Bahrain, all backed by its in-country 24/7 CREST SOC certification.

Comprehensive Cybersecurity Solutions for Every Business Size

ZENDATA's Compliance Packages provide a scalable and cost-effective approach to cybersecurity, helping SMEs and larger enterprises alike achieve compliance and enhance their security posture.

Affordable Cybersecurity for SMEs

With prices starting as low as $25 per month per asset, ZENDATA's cybersecurity packages make regulatory compliance accessible without compromising security.

As cybersecurity regulations evolve, ZENDATA remains committed to empowering businesses in Bahrain with cutting-edge, CREST-certified solutions that ensure compliance and resilience against cyber threats.

CYBLE RECOGNIZED AMONG EXTENDED THREAT INTELLIGENCE SERVICE PROVIDERS IN FORRESTER'S Q1 REPORT

Cyble, a global leader in cybersecurity solutions, has been recognized in Forrester's Q1 2025 report on Extended Threat Intelligence Service Providers (ETISPs), solidifying its position as one of the most trusted names in the industry. This recognition is a testament to Cyble's unwavering commitment to innovation, excellence, and delivering actionable threat intelligence.

The Importance of Extended Threat Intelligence Services

In the contemporary cybersecurity landscape, traditional security measures such as firewalls and anti-virus software are often insufficient to combat sophisticated cyberattacks. Threat actors have evolved their techniques, exploiting vulnerabilities with unprecedented precision and creativity. Thus, extended threat intelligence services have become vital components of any robust security strategy. These services empower organizations to monitor the threat landscape, identify potential risks proactively, and implement defensive measures before threats can escalate.

Extended threat intelligence not only helps organizations respond to immediate threats but also provides insights into the broader threat ecosystem. By understanding adversarial tactics, techniques, and procedures (TTPs), businesses can anticipate potential attacks, build resilience, and allocate resources effectively.

Key Benefits of Extended Threat Intelligence

Proactive Risk Mitigation

One of the standout advantages of extended threat intelligence is its ability to preemptively address potential threats. By leveraging real-time data and predictive analytics, Cyble's solutions empower enterprises to identify risks before they escalate into significant incidents. This proactive approach is critical in mitigating damage and reducing downtime.

Comprehensive Coverage

Extended threat intelligence services go beyond surface-level monitoring. By focusing on adversaries, exposures, vulnerabilities, and critical targets, Cyble delivers a holistic approach to threat intelligence. This ensures organizations can handle all facets of the threat landscape, from identifying malicious actors to addressing infrastructure vulnerabilities.

Global Expertise

With operations across multiple continents, including the U.S., Australia, Singapore, India, and Europe, Cyble provides localized insights coupled with global expertise. This unique blend allows

clients to effectively navigate regional cyber threat challenges while benefiting from a global perspective on emerging trends.

Enhanced Decision-Making

Access to detailed and accurate threat intelligence enables organizations to make informed decisions about their security posture. By understanding the risks they face, businesses can prioritize their cybersecurity investments, ensuring optimal resource use.

These benefits underscore the essential role that extended threat intelligence services play in safeguarding organizational reputation, managing risks, and making informed strategic decisions.

Cyble's Comprehensive Threat Intelligence Offerings

Cyble's position as a leader in the extended threat intelligence space is built on its commitment to delivering cutting-edge solutions that address today's most pressing cybersecurity challenges. The company's advanced offerings are tailored to empower organizations with the insights and tools they need to stay ahead of ever-evolving cyber threats.

Proactive Threat Mitigation Through Cyble Vision

Cyble Vision, the company's flagship threat intelligence platform, delivers unparalleled visibility into the deep, dark, and surface web. It enables organizations to proactively identify and mitigate risks such as exposed credentials, malicious domains, and vulnerabilities. The platform's AI-driven capabilities ensure swift detection and actionable insights, significantly reducing the time to respond to potential threats.

By continuously monitoring online ecosystems, Cyble Vision equips organizations with the ability to detect even the most subtle indicators of compromise. This ensures that businesses remain a step ahead of cyber adversaries, protecting both their digital and physical assets.

Holistic Risk Management with Cyble's Attack Surface Management

Cyble's Attack Surface Management (ASM) solution provides organizations with an end-to-end view of their digital footprint, identifying exposed assets and vulnerabilities before they are exploited by threat actors. By continuously monitoring and analyzing attack surfaces, Cyble helps businesses maintain a robust cybersecurity posture and reduce their exposure to risks.

With the increasing complexity of digital infrastructures, the need for comprehensive ASM has never been greater. Cyble's solution simplifies this process by offering actionable recommendations and seamless integration with existing security frameworks.

Tailored Solutions for Industry-Specific Challenges

Recognizing that different industries face unique threats, Cyble offers tailored solutions for sectors like financial services, healthcare, and government. These sector-specific services address challenges such as regulatory compliance, protection of sensitive data, and defense against nation-state actors. Cyble's expertise in understanding and addressing these challenges ensures comprehensive protection for its clients.

Cyble's Core Strengths in Extended Threat Intelligence

The Forrester report highlights several areas where Cyble excels, making it a favored choice for organizations globally. These strengths are attributable to Cyble's advanced technology, AI-powered platforms, and deep industry expertise. Key areas where Cyble stands out include:

Identifying Impersonations of Company Resources

Impersonation attacks, such as phishing campaigns, fake domains, and fraudulent social media accounts, pose significant threats to organizational reputation, financial stability, and customer trust. Cyble utilizes advanced AI-driven threat detection to identify and mitigate impersonation attempts proactively, protecting organizations from potential brand damage and operational disruption.

Enabling Threat Hunting and Modeling

Cyble equips organizations with powerful threat-hunting capabilities, enabling them to detect and respond to potential threats before they escalate. Through its advanced platform, Cyble supports businesses in modeling potential attack scenarios, simulating cyberattacks, and identifying vulnerabilities in their security posture. This proactive approach ensures that organizations are always prepared for the evolving threat landscape, reducing the risk of data breaches and cyberattacks.

Identifying Exposed Proprietary Information and Intellectual Property (IP)

Protecting intellectual property (IP) and proprietary information from theft and unauthorized access is paramount. Cyble's platform excels at discovering exposed data and vulnerabilities, ensuring businesses can secure their sensitive information quickly. By identifying potential leaks of proprietary data, Cyble enables organizations to minimize the risk of IP theft and maintain their competitive edge.

These core strengths, powered by Cyble's AI and machine learning capabilities, enhance organizational threat detection, reduce response times, and improve overall cybersecurity efficacy.

The Role of AI in Cyble's Success

Artificial intelligence is central to Cyble's success. By automating the analysis of vast datasets, AI enables organizations to identify patterns, respond to incidents quickly, and anticipate future risks. Cyble's AI-driven platforms provide real-time, actionable insights, enabling businesses to make informed decisions about their cybersecurity strategies.

AI also allows Cyble to tailor its services to meet the unique needs of different industries. Understanding the specific

challenges faced by sectors such as banking, healthcare, and government enables Cyble to provide specialized, industry-specific threat intelligence solutions. This specialization strengthens Cyble's position as a trusted partner for organizations worldwide, offering them the tools they need to protect their digital ecosystems from evolving threats.

Access the Cyble Annual Threat Landscape Report 2025

For organizations seeking deeper insights into the cybersecurity landscape, Cyble's Annual Threat Landscape Report 2025 is an invaluable resource. This comprehensive report provides a detailed analysis of the year's most significant cyber threats, emerging trends, and predictions for the future. Leveraging data and insights from the report helps businesses better understand the evolving threat landscape and take proactive steps to defend against cyberattacks.

The report delves into key attack vectors, advanced threat actor tactics, and industry-specific vulnerabilities. By equipping organizations with this knowledge, Cyble empowers them to build more resilient security frameworks and adapt to the rapidly changing cyber threat environment.

Download the Cyble Annual Threat Landscape Report 2025 to discover actionable strategies for navigating today's complex threat environment. The report covers emerging attack vectors, evolving threat actor tactics, and much more, equipping organizations with the knowledge they need to stay ahead of potential risks.

Conclusion

Cyble's recognition in Forrester's Q1 2025 report marks a significant milestone, underscoring the company's position as a leader in the extended threat intelligence arena. By emphasizing innovation, proactive security, and client empowerment, Cyble continues to set the standard for excellence in cybersecurity. The company's AI-powered platform and comprehensive threat intelligence solutions help organizations stay ahead of emerging risks, mitigate cyber threats, and safeguard their digital assets.

As businesses continue to navigate the complexities of the digital landscape, Cyble remains dedicated to providing the tools and insights necessary to combat the growing threat of cybercrime.

CYBERARK AND SENTINELONE TEAM UP TO ENABLE STEP CHANGE IN ENDPOINT AND IDENTITY SECURITY

CyberArk, the identity security company, announced a new integration with SentinelOne's AI-powered cybersecurity platform, SentinelOne Singularity, to protect against privileged access misuse. Integrating the two cyber leaders' platforms brings together the robust endpoint detection and response capabilities of SentinelOne's market-leading Singularity Endpoint solution and CyberArk Endpoint Privilege Manager. The result is a comprehensive security framework that accelerates threat identification and response with unified AI-enhanced security analytics.

"SentinelOne recognizes that cybersecurity is a team sport," said Melissa K. Smith, Vice President, Strategic Technology Partnerships and Initiatives, SentinelOne. "Our integration with CyberArk brings together two market leaders in endpoint security and identity protection and empowers

customers to reduce the risk of privileged identity attacks in an open, flexible way."

The integration also brings new CyberArk identity data into SentinelOne Singularity for AI SIEM and XDR use cases, giving mutual customers greater context and correlation for threat detection and response, threat hunting, investigations and automation.

Clarence Hinton, Chief Strategy Officer, CyberArk, said: "In a multi-cloud world, organizations are looking for new ways to secure identities and must prioritize implementing identity-centric endpoint security controls and system hardening to prevent cyberattackers from gaining a foothold. Through our integration with SentinelOne, we help customers detect and prevent downstream attacks, like privileged credential theft and ransomware. This collaboration uses the power of AI to bring together the complementary strengths of EDR and endpoint identity security, enhancing visibility and boosting defenses against attacks that compromise and exploit privileged access."

CYBER THREATS IN 2025: EVOLVING RISKS AND DEFENSE STRATEGIES

HOW BUSINESSES CAN COUNTER DARK WEB-DRIVEN CYBER THREATS WITH PROACTIVE INTELLIGENCE AND CUTTING-EDGE SECURITY MEASURES.


"MONITORING THE DARK WEB IS ESSENTIAL FOR DISCOVERING STOLEN CREDENTIALS, COMPROMISED PAYMENT INFORMATION, AND NEW FRAUD SCHEMES BEFORE THEY CAN BE USED"

Cyber threats are evolving at an unprecedented pace, posing increasing risks to businesses worldwide. The Middle East, in particular, has emerged as a significant target due to its rapid digital transformation and strategic economic positioning. To delve deeper into these pressing cybersecurity concerns, **Ahmad Halabi, Managing Director of Resecurity Inc** spoke to Sandhya D'Mello, Technology Editor at CPI Media Group on the latest dark web-driven cyber threats, the role of AI in cybercrime, and how organizations can fortify their defenses with proactive threat intelligence solutions.

Cyber threats targeting businesses have evolved significantly, with dark web-driven risks becoming more sophisticated. From AI-based malware and phishing attacks to ransomware-as-a-service and insider threats, organizations face an increasing cybersecurity burden.

Halabi explores how financial institutions, enterprises, and governments can leverage AI-powered threat intelligence, dark web monitoring, and emerging technologies like blockchain and Zero Trust to protect against identity fraud, account takeovers, and brand exploitation.

With insights from Resecurity, the inteview highlights proactive cybersecurity strategies businesses must implement to safeguard their digital assets in 2025 and beyond.

How have cyber threats targeting businesses evolved globally and in the Middle East, and what are the most critical dark web-driven risks organizations face in 2025?

Cyber threats for businesses have significantly advanced worldwide and in the Middle East. Attackers are now utilizing advanced methods like AI-based malware, AI-based hyper-personalized multi-modal phishing, supply chain attacks, and deepfake social engineering. In 2025, risks associated with the dark web are expected to present some of the most serious threats, such as the sale of stolen credentials, insider threat services, and ransomware-as-a-service. Organizations are increasingly challenged by the expanding underground cybercrime ecosystem,

> "REGULATORY COMPLIANCE DOES NOT EQUATE TO SECURITY—CYBERCRIMINALS EVOLVE FASTER THAN REGULATIONS, REQUIRING CONTINUOUS ADAPTATION"

where threat actors collaborate and share attack tools, enabling even novice hackers to carry out high-impact breaches. Solutions like Resecurity's Context Threat Intelligence (CTI) platform tackle these risks by providing dark web monitoring, predictive analytics, and real-time threat intelligence, helping businesses proactively identify and address threats before they escalate. To strengthen their defense against these emerging cyber threats, organizations must adopt continuous threat intelligence and advanced cybersecurity strategies, given the dynamic and fast-changing threat landscape.

With the rapid growth of digital payments and fintech, how can financial institutions leverage dark web monitoring and advanced fraud prevention techniques to combat cybercrime?

As digital payments and fintech proliferate, financial institutions must implement proactive cybersecurity measures to address constantly changing cyber threats. Monitoring the dark web is essential for discovering stolen credentials, compromised payment information, and new fraud schemes before they can be used against fintech and their users. Sophisticated fraud prevention strategies, such as AI-based transaction analysis, behavioral biometrics, and real-time threat intelligence, allow institutions to identify irregularities and prevent unauthorized access. Solutions like Resecurity's Fraud Prevention Platform combine ongoing monitoring of cybercriminal activities with real-time threat assessments to assist financial organizations in predicting fraud tactics and effectively reducing risks. By combining dark web intelligence with machine learning-driven fraud detection, financial institutions can enhance their security, minimize financial losses, and uphold trust with their customers and regulators in a more digital economy.

> **"ORGANIZATIONS ARE INCREASINGLY CHALLENGED BY THE EXPANDING UNDERGROUND CYBERCRIME ECOSYSTEM, WHERE THREAT ACTORS COLLABORATE AND SHARE ATTACK TOOLS"**

How is AI being weaponized by cybercriminals on the dark web for identity theft, credential stuffing, and phishing attacks, and how can organizations use AI-powered threat intelligence to counter these threats?

Defenders and cybercriminals are engaged in an AI arms race, which the cybercriminals are winning. Cybercriminals on the dark web increasingly leverage AI to automate and enhance identity theft, credential stuffing, and phishing attacks. AI tools enable attackers to craft convincing phishing emails, circumvent standard

> **"DEFENDERS AND CYBERCRIMINALS ARE ENGAGED IN AN AI ARMS RACE, AND CYBERCRIMINALS ARE WINNING"**

security measures with deepfake authentication fraud, and automate extensive credential-stuffing attacks using stolen data. Furthermore, AI-based malware and chatbots effectively deceive victims and collect sensitive information. Organizations must implement AI-powered threat intelligence solutions like Resecurity's Risk platform, which provides real-time monitoring, predictive analytics, and automated threat detection to counter these threats. By utilizing machine learning algorithms to detect suspicious activities, identify compromised credentials, and analyze dark web discussions, businesses can proactively defend against AI-driven cyber threats, thus reducing the likelihood of data breaches and financial losses from fraud and the regulatory fines and liabilities that are associated with falling victim to cyberattacks.

What are the key cyber risks unique to the Middle East, including those stemming from cybercriminal activities on underground forums and illicit marketplaces, and how do they compare with global fraud and brand exploitation trends?

The Middle East faces unique cyber risks driven by geopolitical tensions, economic digitization, and targeted cybercriminal activities on underground forums and illicit marketplaces. Cybercriminals exploit regional financial institutions, energy sectors, and government entities through advanced persistent threats (APTs), ransomware, and data breaches. Additionally, underground marketplaces facilitate the sale of stolen credentials,

phishing kits, and fraud services tailored to regional payment systems and telecom networks. Compared to global trends, the Middle East experiences higher state-sponsored cyber espionage and politically motivated attacks, while fraud and brand exploitation tactics—such as fake domains, counterfeit goods, and deepfake scams—mirror global cybercrime patterns. Organizations in the Middle East must strengthen cyber resilience by adopting advanced threat intelligence, dark web monitoring, and fraud detection strategies to mitigate these evolving threats.

How are governments and regulatory bodies shaping threat intelligence policies, and what role do public-private partnerships play in strengthening cyber resilience against fraud and identity threats?

Governments and regulatory agencies increasingly influence threat intelligence policies by implementing stricter cybersecurity frameworks, requiring real-time threat reporting, and encouraging information-sharing initiatives to tackle fraud and identity threats. Regulations like data protection laws, financial security requirements, and critical infrastructure protections compel organizations to embrace proactive threat intelligence and risk management approaches. However, it is vital to point out that when a company complies with regulations, it does not equate to being secure against cyber threats. Regulations evolve slower than how threat actors continuously evolve their TTPs to counter regulations and security products and policies used by defenders.

When a company Public-private partnerships are essential for bolstering cyber resilience as they foster collaboration among law enforcement, financial institutions, and cybersecurity companies. These alliances allow for real-time intelligence sharing, coordinated responses to emerging threats, and collective actions against cybercriminal networks operating on the dark web. By merging regulatory compliance with cutting-edge threat intelligence solutions, organizations can improve their capabilities to identify, prevent, and respond to sophisticated cyber threats more effectively.

What emerging technologies, such as blockchain, Zero Trust, and AI-driven threat intelligence, are transforming brand protection and fraud prevention efforts in the fight against cybercriminals?

Emerging technologies such as blockchain, Zero Trust security, and AI-based threat intelligence are transforming brand protection and fraud prevention by improving transparency, authentication, and threat detection. Blockchain ensures immutable transaction logs, which help minimize fraud in financial dealings and supply chains by thwarting counterfeiting and unauthorized changes. Zero Trust architecture enhances security through relentless verification, reducing the chances of identity fraud and insider threats. At the same time, AI-driven threat intelligence uses machine learning to spot fraudulent activities, monitor dark web discussions, and anticipate cybercriminal strategies in real-time. By adopting these technologies, organizations can protect their brands, avert data breaches, and effectively confront increasingly advanced cyber threats more efficiently and precisely.

> "AI TOOLS ENABLE ATTACKERS TO CRAFT CONVINCING PHISHING EMAILS, CIRCUMVENT SECURITY MEASURES WITH DEEPFAKE FRAUD, AND AUTOMATE EXTENSIVE CREDENTIAL-STUFFING ATTACKS"

> "BLOCKCHAIN, ZERO TRUST SECURITY, AND AI-BASED THREAT INTELLIGENCE ARE TRANSFORMING BRAND PROTECTION AND FRAUD PREVENTION EFFORTS"

What proactive threat intelligence strategies should businesses implement to detect and mitigate dark web threats, account takeovers, and identity fraud before they escalate?

Businesses should adopt proactive threat intelligence approaches, including ongoing dark web monitoring, AI-based fraud detection, and multiple security controls to identify and address cyber threats before they worsen or become victimized by them. Organizations can pinpoint compromised credentials and emerging fraud tactics in real-time by monitoring underground forums, illegal marketplaces, and data breaches. AI-enhanced behavioral analytics can recognize anomalies indicative of potential account takeovers, while identity verification methods, like biometric authentication and adaptive risk scoring, bolster fraud prevention efforts. Moreover, implementing Zero Trust principles guarantees continuous authentication and restricts unauthorized access. Utilizing advanced threat intelligence platforms such as Resecurity's Context CTI allows businesses to obtain actionable insights, automate threat detection, and proactively manage risks, minimizing the risk of dark web-fueled cybercrime.

HUAWEI'S STRATEGIC ADVANCEMENTS IN AI SECURITY AND SUPPLY CHAIN MANAGEMENT SECURITY

ENG. ABDULAZIZ AL NUAIMI, CHIEF SECURITY OFFICER, HUAWEI UAE

Securing Artificial Intelligence (AI) systems and supply chains has become a critical concern for global technology companies and Huawei, a global ICT leader, is tackling these challenges head-on and leveraging its expertise to establish industry standards in AI security and supply chain resilience.

AI Security: Addressing Complex Challenges

AI's transformative potential is accompanied by inherent risks such as data breaches, adversarial attacks, and algorithmic biases. Acknowledging these vulnerabilities, Huawei has crafted a multi-layered strategy to safeguard AI systems.

Central to Huawei's AI strategy is a steadfast commitment to ethical practices. The company designs AI frameworks that prioritize transparency, privacy, and accountability. It integrates Explainable AI (XAI) techniques to ensure decision-making processes are understandable and unbiased, thereby fostering trust among users and stakeholders.

Huawei has also harnessed the power of AI to bolster its cybersecurity defenses. By deploying advanced threat detection systems, its technology analyzes vast amounts of data to identify and neutralize potential threats in real time, providing robust protection for its AI solutions.

Huawei's efforts extend beyond its internal operations. Through initiatives like the Huawei Cyber Security Transparency Center, the company collaborates with academia, industry experts, and policymakers to advance AI security research and address emerging challenges. These measures underline Huawei's commitment to creating secure, scalable, and trustworthy AI systems that can withstand the complexities of the modern digital ecosystem.

Securing the Global Supply Chain

In the interconnected world of global supply chains, vulnerabilities such as counterfeit components, tampering, and cyberattacks pose significant risks. To mitigate these challenges and protect the integrity of its supply chain, Huawei has implemented a comprehensive security framework.

Huawei employs blockchain technology to enhance supply chain traceability, ensuring every component and process in its network is authenticated, thus reducing the risk of counterfeit products and unauthorized modifications.

Huawei also enforces stringent supplier verification protocols, requiring partners to adhere to its cybersecurity standards. Regular audits and compliance checks are conducted to maintain the integrity of the supply chain.

Huawei incorporates secure-by-design principles into its hardware and software, ensuring resilience against potential cyberattacks. AI technologies are also deployed to predict and mitigate supply chain disruptions, enhancing overall reliability.

By aligning with international frameworks like ISO 28000 and contributing to global cybersecurity policy development, Huawei demonstrates its commitment to fostering a secure and standardized supply chain ecosystem.

Setting Industry Benchmarks

Huawei's proactive approach to AI and supply chain security establishes it as a leader in the global technology landscape. By combining cutting-edge innovation with robust security measures, the company not only protects its operations but also contributes to the broader effort to secure the digital future.

As cyber threats become increasingly sophisticated, Huawei's initiatives serve as a model for how technology companies can balance innovation with security. Its commitment to transparency, collaboration, and ethical practices underscores the importance of building trust in an increasingly digital world.

For industries and organizations navigating the complexities of AI and global supply chains, Huawei's efforts underscore the critical need for vigilance, resilience, and collaboration in ensuring a secure and sustainable technology-enabled future.

VENDOR LOCK-IN HAS LEFT ENTERPRISES VULNERABLE TO MAJOR SECURITY ATTACKS, SAYS CLOUDFLARE CSO

GRANT BOURZIKAS, CSO AT CLOUDFLARE, HAS SAID THAT VENDOR LOCK-IN IS A CRUTCH THAT ORGANISATIONS NEED TO REMOVE IN ORDER TO ELIMINATE THEIR CHANCES OF BEING COMPROMISED BY THREAT ACTORS. IN AN EXCLUSIVE OP-ED FOR TAHAWULTECH.COM, BOURZIKAS HAS CALLED FOR ENTERPRISES TO START THEIR 'SECURITY TRANSFORMATION' NOW.

Vendor lock-in is a crutch that will lead to increasing breaches in 2025 – organisations must start their security transformation journeys.
The deeply rooted foothold that vendors have in organisations' environments has become one of the main drivers of complexity. The bottom line is that complexity creates chaos, and chaos distracts from the real priorities when it comes to securing an organisation.

Being held hostage by a vendor, to a point where moving off of them seems impossible, is the moment they begin to help shift the balance of power back in favour of threat actors. The hyper-focus on "digital transformation" over the past few years – implementing a myriad of new tools and vendors across the organization to rapidly innovate – has left security in the dark.

In 2025, we will feel the full weight of having fallen victim to the cycle: shiny new tools, Wall Street's buy-in, rush to implement, repeat. We must now shift focus to "security transformation," and begin to remove the tools and vendors that are causing complexity vs. furthering innovation.

In 2025, disinformation will transcend the Internet and social media, and move to poison and taint AI models.
Information sharing exists at an order of magnitude faster, and more efficient than ever before. And in the world of AI, data is the only currency and organisations that have the most will win – but quantity doesn't always equal quality. AI on its own will not solve the world's most critical problems.

The successful implementation and use of AI depends on data. But as disinformation continues to plague society, it will begin to trickle into AI models that are critical to making decisions – e.g., calculating goods needed to restock grocery store shelves, diagnosing sick patients or analyzing market trends to share financial risks with bankers.

Broad brush cyber regulations legislated with good intent will have a reverse effect in 2025 – creating complexity and having no real impact on stopping attacks.
In the past few years we have witnessed a cadence of record shattering, significant breaches that have drawn the eye of regulators. But while their attempts to raise the security resiliency of organizations are aimed to be helpful, they are often knee jerk reactions that require unrealistic efforts.

This is a complete misstep, with much of today's regulatory efforts ineffective and not focused on the most critical aspects of security controls. Regulators still fail to recognize what will make the biggest difference in moving the needle towards immutable infrastructure.

In 5-10 years there will only be two types of companies: Those that leveraged AI to innovate, and those that no longer exist.
With this harsh reality, CISOs must figure out how to be an enabler of AI, not a blocker. But with AI still in its infancy, very few have a strong understanding of the technology or the risks it may present... leading to extremely low levels of confidence that their organization is well-prepared.

The lack of understanding around AI, is ultimately giving threat actors a leg up.

MANAGING THE THIRD-PARTY BLINDSPOT FOR DORA

Andre Troskie, EMEA Field CISO, Veeam

The financial service industry is no stranger to stringent regulation. Unlike other sectors that have scrambled to comply with legislation such as NIS2, FS organizations are comparatively pretty diligent when it comes to data resilience and cybersecurity. Having operated under some of the strictest regulatory standards for some time, for most, DORA compliance should be manageable - for internal operations that is.

Despite the confidence that many FS organizations likely have in their ability to comply with DORA audits and reporting, they can't afford to take their eyes off the ball. DORA compliance extends beyond internal procedures, covering third-party service providers as well. It's here where most organizations risk tripping up in the initial stages of DORA enforcement. With consequences ranging from significant fines to brand and reputational damage, it's an issue that organizations can't afford to overlook.

Well prepared?

Unlike other sectors that also have to comply with NIS2, financial services organizations by necessity are typically further ahead of the curve when it comes to regulatory compliance. For

many, DORA's requirements will have been about building on (and proving) the strength of the foundations already in place. The main focus on DORA for financial services will likely instead be on operational resilience testing, ensuring internal awareness of different scenarios and their risk impacts.

Most financial institutions and banks will have felt confident in their scenario-based testing and, by extension, their compliance with DORA when the deadline passed this January. And if the scope of DORA didn't cover beyond internal organization compliance, they would be right. Unfortunately for most, DORA extends to cover all of an organization's third parties and supply chains - creating the risk of a pretty large potential blindspot.

Time to put the work in

Financial services organizations can do all the work they want ensuring internal compliance to DORA but unless their third-party and supply partners are also compliant, they will fail regardless. And these are no small stakes. According to EY's Global Third-Party Risk Management Survey, in the US alone, 98% of financial services organizations have partnerships with third-party vendors. Although they may not realize it, third parties are one of the biggest risks to FS organizations when it comes to DORA compliance.

Sadly, there is no quick fix. At the very minimum, every bank and financial institution in every EU Member State that falls under DORA is going to have to renegotiate many Service Level Agreement (SLA) with existing and new third-party partners. Financial services organizations can't afford to be under any illusions, this will be a necessary but significant piece of work. Cementing DORA compliance as a pre-requisite will be essential for continued DORA compliance but will require collaborative work from across businesses. Security, risk management, and legal teams will all need to band together to pull this off.

DORA's double-duty for data resilience

Of course, even having DORA compliance confirmed amongst your third-party providers won't make your organization completely invulnerable to cybersecurity threats. But, it will put you in good stead when it comes to recovering from an attack. After all, regulatory compliance has never equalled complete security. DORA is more of an exercise in operational resilience improvement, which is a key piece of the puzzle for recovery from cyber attacks.

But this doesn't mean that compliance should be an afterthought. For financial services organizations to achieve compliance with DORA and secure their third parties, they'll need to dedicate around-the-clock attention. It's not a one-and-done deal, it will be a reiterative and continual process to achieve compliance consistently across all providers. That is if they want to avoid the chaos that 11,000 Starbucks stores dealt with when their third-party cloud provider was taken out by a ransomware attack last winter.

Sure, it'll require a significant amount of resources to completely map out all of your third-party providers and introduce those contractual safeguards, but it'll serve double duty. Not only will you ensure compliance, but you'll also cement robust data resilience as a backbone of your organization's incident response plans. Last year alone, the cost of downtime for financial services organizations was $152 million. So, if the worst does happen, you'll want to be able to bounce back as quickly as possible or face adding to that number this year.

There are of course other benefits to compliance, primarily the avoidance of any consequences. DORA in particular comes hand in hand with European Supervisory Authorities (ESAs) that will regularly check for compliance and hand down any relevant repercussions. For financial services, if their external critical software providers don't comply in time, they could face anything from a fine of 2% of their annual turnover to criminal charges.

So yes, DORA compliance can't bulletproof you against every threat out there, but being able to prove that everything is in place and that it all works within the defined time frames, will set you up to recover as swiftly as possible from cyberattacks. And, perhaps more prudently, it'll prevent you from incurring any of the severe consequences attached to non-compliance. Organizations need to step it up a notch when it comes to DORA compliance and, most importantly, ensure their third parties are along for the ride.

WHY COLLABORATION IS KEY TO DISRUPTING THE ECONOMICS OF CYBERCRIME

DEREK MANKY, CHIEF SECURITY STRATEGIST & GLOBAL VP THREAT INTELLIGENCE, BOARD ADVISOR, THREAT ALLIANCES AT FORTIGUARD LABS

Businesses worldwide are embracing digital evolution. Yet cybersecurity implications inevitably emerge as technologies evolve and push us into a new era of connectivity.

Adopting new technologies, devices and platforms increases potential points of compromise, widening an organization's attack surface. Having more digital systems to configure, integrate and manage leads to greater complexity and an increased likelihood of error.

And more systems mean more data is being collected, stored and analyzed, which creates new risks. Given the myriad of changes organizations face, it's no surprise that 87% of enterprises report experiencing at least one breach in 2023.

Meanwhile, cybercriminals are expanding collaborative efforts within their ecosystem as they look to exploit and capitalise on weaknesses in organizations and their targets.

Malicious actors harnessing new technologies for cybercrime

As the threat landscape continues to evolve and malicious actors harness new technologies like artificial intelligence (AI) to increase the volume and velocity of the threats they deploy, they have effectively built a resilient and profitable ecosystem that continues to elevate risk to businesses and critical infrastructure.

This evolution presents a very real challenge for defenders everywhere, creating a situation that is exceedingly difficult to course-correct. As the state of cybersecurity continually shifts, one thing is clear: no single organization alone can effectively disrupt cybercrime. By working together and sharing intelligence across industries and borders, we're collectively better positioned to fight against adversaries.

Public-private collaborations like the World Economic Forum's Cybercrime Atlas project offer us vital insights and a practical, scalable partnership model.

The Cybercrime Atlas, which has been in operation for one year, is a collaborative effort to build an action-oriented, global knowledge base on cybercrime to support the mitigation and disruption of adversary activities.

Building on expertise from the Forum's Partnership Against Cybercrime, the initiative is developing a comprehensive picture of the cybercrime landscape that details criminal operations, shared infrastructure and networks, all of which helps law enforcement and government agencies take down global cybercrime groups and their infrastructure.

87%
Enterprises report experiencing at least one breach in 2023

The far-reaching impacts of cybercrime

When an organization suffers a breach, the impacts are often far-reaching and time-consuming to remedy. The time between vulnerability discovery and exploitation is also shrinking, with bad actors exploiting new vulnerabilities in under five days – 43% faster than before.

First, remediating cyber incidents frequently requires an extraordinary amount of time and money. More than 60% of leaders said it took longer than a month to recover from a cyberattack, and 53% indicated that breaches cost their enterprise more than $1 million in lost revenue, fines and other expenses.

In addition, board members and executives are increasingly being held accountable when breaches happen, with 34% receiving financial penalties.

Many organizations do not have the necessary resources to protect a growing attack surface against an increasingly sophisticated threat landscape. Leaders say the following attributes contribute to breaches: an IT and security staff without the appropriate skills and training (58%), a lack of general cyber awareness among employees (56%) and a lack of cybersecurity products (54%).

Navigating future cybersecurity challenges

When faced with an increasing number of cyberattacks, many organizations think in terms of what additional security tools they need. However, building alliances is one of the most effective – and frequently overlooked –actions organizations can take to address the urgent challenge of cybersecurity and combat cybercriminals.

Building relationships and exchanging information fosters trust, and when public and private institutions have more trust in one another, more intelligence can be shared in an effort to not just keep pace with but also stay ahead of cyber threats.

Looking ahead, adversaries will embrace bigger and bolder attacks, adding new tactics to their toolboxes, setting their sights on fresh targets and launching meticulously planned attacks crafted to fool even the most savvy end-user.

Threat actors will continually advance their efforts, making it essential that organizations adjust accordingly, taking a comprehensive and collaborative approach to risk management. As the saying goes: "Change starts from within." Every enterprise needs to first strengthen its own cyber resilience through efforts like building a culture of cybersecurity, identifying ways and implementing programmes to shrink the cyber skills gap and dismantling internal silos to increase cross-department collaboration related to cybersecurity.

Embracing these shifts enhances the organization's security posture and is the first step to the entity being able to more effectively collaborate in the larger fight against cybercrime. Then, the way forward is systemic disruption of this ecosystem.

Laying the foundation for the systemic disruption of cybercrime

To address the industry's challenges with disruption, broad and collaborative

efforts, including the World Economic Forum Cybercrime Atlas initiative, are in motion and are already gaining traction to disrupt these criminal ecosystems systemically at scale.

The Cybercrime Atlas was created to build a shared knowledge base to disrupt cybercrime. This collective disruptive force of education, resilience and law enforcement offers the way forward to start minimizing risk to business and disrupting the very economy that is fuelling the campaigns from the adversary.

The atlas is also a source for evidence-based recommendations to shape improvements to public policy and practical guidance to enhance operational collaborations that counter cybercrime. This will make the internet a higher risk environment for cybercriminals.

Effective partnerships can help us identify choke points on the attacker chess board, finding opportunities to meaningfully disrupt cybercrime operations. But what makes these partnerships successful, and how can we emulate existing successful collaborations?

To expand on and introduce new collaborative efforts, we must examine common traits of existing effective partnerships and frameworks and apply those to future work.

The World Economic Forum's Centre for Cybersecurity recently released its Disrupting Cybercrime Networks collaboration framework, which articulates three core pillars of collaboration relating to anti-cybercrime efforts.

First, organizations must have an incentive to participate, such as a clear mission and impact. Next, the effort must have a solid governance structure. Finally, having the proper resources – ranging from common taxonomies and data normalization practices to technology and people – to set up, maintain and accelerate the partnership is paramount.

The first year of the Cybercrime Atlas initiative also offers us a roadmap for the systemic disruption of cybercrime, as detailed in the group's impact report.

During this time, Cybercrime Atlas contributors shared more than 10,000 community-vetted and actionable data points, created seven comprehensive intelligence packages on emerging threats to distribute broadly to law enforcement agencies and supported two cross-border cybercrime disruption efforts.

Knowing that there are inherent hurdles often associated with threat intelligence sharing, the Cybercrime Atlas group made deliberate decisions to remove those barriers to facilitate the exchange of insights.

For example, Cybercrime Atlas relies strictly on open-source intelligence, eliminating privacy concerns and facilitating frictionless information sharing. The group draws expertise from defenders worldwide and targets cybercrime globally, as most cybercrime groups are transnational and have multiple operation centres.

Finally, the Cybercrime Atlas research findings pinpoint where threat actors and their operations are the most vulnerable, which paves the way for domain takedowns, communications account closures, crypto wallet seizures and more.

Collaborative efforts to disrupt cybercrime will only become more critical as the threat landscape intensifies.

Effectively halting cybercrime requires a global and collaborative approach. By embracing best practices and proven frameworks for anti-adversary partnerships, we can jump-start new and enhance existing initiatives, collectively creating a safer digital world for all.

عالم الذكاء الاصطناعي
EVERYTHING
— GLOBAL —

4 FEB 2025
Ai Everything Summit | 10 am - 5 pm
THE ST. REGIS SAADIYAT ISLAND RESORT | ABU DHABI

5 – 6 FEB 2025
Exhibition Showcase | 10 am - 5 pm
DUBAI EXHIBITION CENTRE (DEC) | EXPO CITY

POWERING GLOBAL COLLABORATIONS IN THE NEW AI ECONOMY

500+	150+	60+	200+	500+
EXHIBITORS	INVESTORS	COUNTRIES	SPEAKERS	CHIEF AI OFFICERS

From 4-6 February, the world's most influential tech policymakers, enterprises, corporate executives, investors, academics and award-wining startups will unite in the two emerging AI super hubs - Abu Dhabi and Dubai.

REGISTER NOW
aieverythingglobal.com

ACCELERATED BY
GITEX GLOBAL

/AiEverythingGLOBAL

MICROSOFT NAMES SAMER ABU-LTAIF PRESIDENT FOR EUROPE, MIDDLE EAST AND AFRICA

WITH OVER 34 YEARS OF EXPERIENCE IN TECHNOLOGY AND BUSINESS GROWTH, ABU-LTAIF WILL LEAD MICROSOFT ACROSS MORE THAN 120 MARKETS IN EMEA, DRIVING DIGITAL TRANSFORMATION FOR CUSTOMERS AND PARTNERS IN THE ERA OF AGENTIC AI.

Microsoft has announced the appointment of Samer Abu-Ltaif as the President of Microsoft Europe, Middle East, and Africa (EMEA). Abu-Ltaif succeeds Ralph Haupter, who will assume the role of President, of the newly formed Microsoft Small, Medium Enterprises and Channel partner organization.

In his new role, Abu-Ltaif will leverage his extensive experience in driving digital transformation and fostering collaboration to strengthen Microsoft's presence in the EMEA region. Spanning over 120 markets, he will play a pivotal role in empowering customers and partners to harness the transformative potential of AI, enabling them to achieve more and help drive innovation and sustained economic growth across the region.

Abu-Ltaif brings a wealth of expertise, having recently served as President for Central and Eastern Europe, Middle East and Africa (CEMA). Under his leadership, Microsoft deepened partnerships with strategic service providers, expanded its regional footprint, and delivered enhanced value to customers and partners across three continents.

During his two-decade tenure at Microsoft, Abu-Ltaif has spearheaded transformative initiatives that have solidified Microsoft as a key partner in advancing regional priorities. This includes achievements like the launch of Microsoft's first datacenter on the African continent in South Africa, datacenters in the UAE, Qatar and Poland, a recently announced Global Engineering Development Center in the UAE, and planned datacenter regions in Greece and Saudi Arabia as well as the upcoming datacenter region in Kenya. He also played a pivotal role in the opening of Microsoft Africa Development Center in Kenya, and the company's $1.5 billion investment in Abu Dhabi's G42, aimed at accelerating AI innovation globally.

Abu-Ltaif has also been a key advocate for workforce development through skills training programs such as Tomoh, AthkaU, TechDev, Africa Development Bank partnership, Digital Heartbeat and Tawar w Ghayar that have empowered millions of people across the region by equipping current and future generations with the tools and opportunities needed to thrive in the digital age. His unwavering commitment to sustainability has fostered impactful collaborations with governments, businesses, and startups, advancing the region's sustainability agenda and driving meaningful change.

Based in UAE, Abu-Ltaif has held several senior leadership roles at Microsoft, including President for the Middle East and Africa, and Regional Director for the Gulf region. He holds an MBA in Leadership and Sustainability and a degree in Computer Science Studies from the American University of Beirut.

SHINICHI 'SAM' YOSHIDA NAMED PRESIDENT AND CEO FOR CANON EMEA

Canon EMEA, a global provider of imaging, print technologies and services, announced Shinichi 'Sam' Yoshida as President & CEO for Canon Europe, Middle East and Africa (EMEA), succeeding Yuichi Ishizuka who is retiring after seven years in the role and a successful 44-year career with Canon.

Sam Yoshida was previously based in the USA where he held the position of Executive Vice President and General Manager of the Marketing Strategy Unit, Chairman and Chief Executive Officer of Canon Solutions America, Inc. and Canon Financial Services, Inc. He will assume his new responsibilities as President & CEO of Canon EMEA from March 1.

Yoshida takes over a regional sales organisation which has operations in 120 countries, employs approximately 12,300 people and contributes about a quarter of Canon's global revenues annually.

Yoshida is tasked with bolstering and growing existing core businesses while capitalising on the brand's reputation for imaging and printing technology and solutions expertise to expand into new areas such as B2B Imaging, Industrial and Commercial Printing and Information Management Solutions. He brings a wealth of expertise including manufacturing, innovation and recycling having been part of the original team that established Canon Virginia, Inc., Canon's major manufacturing site in the Americas.

"Canon is the market leader in imaging and print technologies with millions of customers throughout EMEA; this diverse and exciting region is full of opportunity and I am honoured to be leading the business through the next phase of innovation and growth." says Yoshida.

Yuichi Ishizuka, President & CEO of Canon EMEA, held senior positions globally over his 44-year career, including in Japan, USA, and Canada. During his successful career a notable highlight was his pioneering launch of the world-renowned Cinema EOS range in the US, which has revolutionised film shooting and created mainstay video products.

INTERSEC 2025 WELCOMED RECORD NUMBER OF EXHIBITORS CULMINATING IN LARGEST EXHIBITION TO DATE

The 26th edition of Intersec, the world's biggest business event mapping the future of security, safety and fire protection, has showcased a record number of exhibitors, representing 61 countries, with the largest edition of the event occupying 61,000 sqm of space, a 20% year-on-year increase at the Dubai World Trade Centre (DWTC).

The event, which was held under the patronage of Sheikh Mansoor Bin Mohammed bin Rashid Al Maktoum, and concluded last month, welcomed 47,300 visitors from 142 countries, showcasing cutting-edge technologies and critical solutions across five key sectors: Commercial & Perimeter Security, Fire & Rescue, Safety & Health, Cyber Security, and Homeland Security & Policing, in line with the show theme 'Mapping the Future of Security, Safety, and Fire Protection.'

Wajahat Hussain, Show Manager, Messe Frankfurt Middle East, said: "The team and I are thrilled to have welcomed an unprecedented gathering of industry professionals from around the world. Intersec has once again proven to be the premier platform where global leaders, innovators, and experts converge to exchange knowledge, forge partnerships, and explore cutting-edge advancements that are shaping the future of safety, security, and fire protection.

"Surpassing previous exhibitor records is a testament to Intersec's growing influence and its pivotal role in driving forward-thinking solutions for a safer, more secure world. This milestone underscores our commitment to fostering collaboration, showcasing pioneering technologies, and setting new benchmarks for excellence in this critically important industry."

This year's new additions included the successful launch of the two-day Intersec Policing Conference, where over 50 expert speakers convened. They included senior law enforcement officials from the Abu Dhabi Police, INTERPOL, the Metropolitan Police and the UAE Financial Intelligence Unit, where discussions focused on topics including policing in a digital era, proactive and productive policing, the future of road safety, strategic automation in policing, drone operations and quantum-led crime, amongst others.

In addition, the CISO Business Briefing was also launched, successfully welcoming the region's top Chief Information Security Officers (CISO) while investigating the key trends, threats and opportunities in information security. H.E Dr. Mohamed Al Kuwaiti, Head of Cybersecurity, UAE Government, provided the opening keynote address.

Another first for the exhibition was a groundbreaking partnership with Ignyte, which saw the launch of the Intersec Startup Arena, providing startups with a unique opportunity to showcase the ideas and solutions disrupting the industry to an audience of industry leaders, government representatives, and top-tier investors, paving the way for startups to achieve strategic partnerships, mentorship, and investment.

Intersec 2025 also bore witness to several MoU signings during the three-day event, including companies such as Abu Dhabi Civil Defence, Nordon, Saudi Sicli, ASIS International, Firestop Contractors International Association (FCIA), Gallagher, Sharjah Civil Defence, NAFFCO, and UXE Security Solutions.

Several industry bellwethers were recognised during the 4th annual Intersec Awards, where individuals, teams and organisations were recognised for setting new standards of excellence in critical industries. Winners on the evening included Dubai Civil Defense, NAFFCO, Dubai Municipality, Ministry of Interior, Emirates Safety Laboratory LLC, and the Telecommunications and Digital Government Regulatory Authority (TDRA).

Intersec 2026 will take place from 12 – 14 January 2026 at the Dubai World Trade Centre.

- 1,209 exhibitors representing 61 countries were showcased at the 26th edition of Intersec, a 9% increase on last year, including a 20% increase in exhibition space
- The exhibitions saw the successful launch of the Intersec Policing Conference and the CISO Business Briefing, an exclusive forum for Chief Information Security Officers to discuss emerging cybersecurity trends and strategies
- This year's show highlighted cutting-edge technology and critical solutions in line with the theme: 'Mapping the Future of Security, Safety, and Fire Protection

GENETEC AT INTERSEC 2025: DRIVING SECURITY INNOVATION ACROSS THE MIDDLE EAST & AFRICA

EXPLORING MARKET GROWTH, DIGITAL TRANSFORMATION, AND AI-DRIVEN SECURITY SOLUTIONS WITH GENETEC'S TOP EXECUTIVES

By Sandhya D'Mello

At Intersec 2025, Genetec, a global leader in unified security solutions, showcased its latest advancements and strategic insights tailored for the evolving security landscape in the Middle East and Africa. With the UAE and Saudi Arabia spearheading digital transformation and Africa emerging as a key market, Genetec's top executives—Andrew Elvish (Vice President of Marketing), Andy Mackay (Marketing Director EMEA), and Quintin Roberts (Regional Sales Manager Africa)—shared their perspectives on industry trends, technological innovations, and the company's expansion strategy.

From Zero Trust security models to AI-driven automation and smart city integrations, Genetec continues to lead the way in modernizing security infrastructure. In these exclusive interviews, the company's leaders discuss the increasing demand for cybersecurity, how Genetec is aligning with regional policies, and its commitment to partner training, market growth, and operational efficiency.

The MENA physical security market, projected to reach $3.0 billion by 2028 with a CAGR of over 7%, is driven by rapid infrastructure growth and rising demand for AI-powered technologies. According to the Genetec State of Physical Security Report 2025, 46% of end users plan to implement AI-powered features in 2025, reflecting a significant shift towards automation and enhanced threat detection.

Interview with Andrew Elvish, Vice President of Marketing, Genetec

How does Intersec 2025 reflect the UAE's rapid growth and evolving policies, and how does Genetec align its global strategy with the region's dynamic market and future trends?

Intersec 2025 is clearly bigger than last year, with more exhibitors, and higher traffic on the show floor, reflecting a growing interest and investment in the market, and signaling that more business is happening, and curiosity is expanding.

Over the last six to seven years, the Middle East market has grown significantly, both for Genetec and on the global stage. The UAE, along with Saudi Arabia, is becoming an increasingly consequential player in the region. A key differentiator is the ability to set and execute long-term strategies, unlike other regions where political cycles disrupt continuity. The region has demonstrated deterministic growth, with clear objectives such as increasing the share of GDP from advanced technology development, including AI, computer science, engineering, and technology sales.

Looking at the exhibition floor, there is a strong synergy between sophisticated technology companies and Middle Eastern buyers, whether end users or government entities. The market's trajectory indicates continued development of both technological and physical infrastructure, which in turn is driving demand for security solutions.

Security is a major focus at Intersec. As sectors like data centers, airports, city-wide developments, hotels, and resorts expand, there is a growing need for high-end security technology. However, the region is not approaching security in an unstructured manner. Regulations like Security Industry Regulatory Agency (SIRA) ensure that security solutions, including Genetec's Security Center software, meet strict compliance standards, allowing for controlled and smart implementation.

From a business and marketing perspective, the Middle East remains a fast-growing market with strong potential for continued expansion over the next two years.

Andrew Elvish, Vice President of Marketing, Genetec

How can entrepreneurs make Zero Trust a top priority in business, especially with the rise of remote work in the UAE? Additionally, how does Genetec ensure Zero Trust is embedded in its security approach?

The key to prioritizing Zero Trust in your business is to develop a cybersecurity strategy built on a Zero Trust architecture. At Genetec, cybersecurity has been a core focus for years. Back in 2015-2016, we took a strong stance against untrustworthy devices, recognizing that physical security systems operate on IP networks with multiple sensors—essentially computers that can be exploited if not secured properly.

Many businesses unknowingly deployed devices without checking if their passwords were changed, if they had backdoors, or if they were cyber-secure. This led to denial-of-service attacks, data

breaches, and other security risks. In response, we blocked unsafe cameras from our platform and have continued to push for higher cybersecurity standards in the industry.

For the UAE and other regions serious about cybersecurity, following best practices is crucial. The real concern isn't just what these cameras or sensors capture; it's the network access they provide.

To fully implement Zero Trust, businesses must move beyond traditional perimeter security models. There should be no assumption of trust within the network—access should only be granted based on strict authentication protocols. This includes using high-reliability authentication, like multi-factor authentication (MFA) with hardware security keys (such as YubiKeys), rather than just passwords.

At Genetec, we enforce these principles rigorously, ensuring our software and network designs align with Zero Trust and defense-in-depth strategies. We also work closely with partners who meet our strict cybersecurity expectations, and we actively educate the industry on the evolving landscape of cybersecurity.

For entrepreneurs, the best way to adopt Zero Trust is to work with vendors and partners who prioritize cybersecurity, implement robust authentication measures, and continuously monitor and update their security protocols to stay ahead of emerging threats.

Genetec operates as a global company with a selective approach to its channel partners. How do you ensure that only qualified integrators deploy your solutions, and why is this level of exclusivity important for customer satisfaction?

> **"FROM A BUSINESS AND MARKETING PERSPECTIVE, THE MIDDLE EAST REMAINS A FAST-GROWING MARKET WITH STRONG POTENTIAL FOR CONTINUED EXPANSION OVER THE NEXT TWO YEARS**
>
> ***ANDREW ELVISH, VICE PRESIDENT OF MARKETING, GENETEC"***

At Genetec, I would say, globally we have 4,000 active partners,we take a highly selective approach when choosing our channel partners because our product, while designed for ease of use, can be deployed in highly sophisticated ways. Our end users expect more than just basic security functions like viewing cameras or controlling access. They require advanced integrations such as identity management, access control with HID Mercury, legacy system plugins, and data visualization.

Given this complexity, it's critical that our partners are well-trained and certified. We do not accept integrators who lack proper certification, even if they bring us a project opportunity. While some may see this as a strict approach, it ultimately ensures the best experience for our customers. We've seen cases where companies worked with non-certified integrators and ended up dissatisfied—not because the technology was flawed, but because the deployment was mishandled.

By maintaining a rigorous partner certification process, we ensure that our solutions are implemented correctly, meeting the high expectations of our end users. This commitment to quality protects both our brand and our customers, ensuring they receive the full value of Genetec's technology.

Interview with Andy Mackay - Marketing Director EMEA, Genetec

How does Genetec navigate traditional business mindsets in the Middle East and Africa, ensuring proactive adoption of its solutions?

One of the most significant changes we've observed in the Middle East and Africa is the shift in decision-making from traditional operations departments to IT departments. This transition is accelerating, particularly in regions like Saudi Arabia, where businesses are moving away from legacy systems and adopting the latest technologies directly.

In this region, there is a strong alignment between market needs and the advanced features and functionalities that Genetec delivers. Unlike some markets that may be hesitant about investing in cybersecurity and advanced security solutions, businesses here recognize the importance of staying ahead of threats. This forward-thinking mindset allows organizations to proactively implement security solutions that not only protect their infrastructure but also ensure long-term resilience.

At Genetec, we focus on educating businesses about the value of proactive security measures rather than reactive ones. By demonstrating how our solutions contribute to reducing security risks, improving operational efficiency, and ensuring compliance with evolving regulations, we help businesses understand that investing in advanced security today prevents higher costs and risks in the future.

What are the key industries and geographical markets driving Genetec's growth in the Middle East and Africa?

Currently, the two major sectors driving Genetec's growth in the Middle East are transportation and smart cities. The rapid expansion of new airports and rail networks across the region is fueling demand for advanced security and surveillance

solutions. Additionally, the development of smart cities is creating a strong need for security infrastructure to manage the movement of people efficiently and securely.

In Africa, there is notable demand in critical infrastructure, particularly in oil and gas and mining sectors, where security solutions play a crucial role in protecting assets and operations.

From a geographical perspective, Saudi Arabia stands out as the fastest-growing market, with significant investments in large-scale infrastructure projects. Alongside Saudi Arabia, the UAE remains a key market for Genetec, given its commitment to adopting cutting-edge security solutions. Additionally, sub-Saharan Africa is emerging as a high-growth region, with businesses and governments increasingly prioritizing cybersecurity and adopting the latest technologies to secure critical assets.

Andy Mackay - Marketing Director EMEA, Genetec

> "AT GENETEC, WE FOCUS ON EDUCATING BUSINESSES ABOUT THE VALUE OF PROACTIVE SECURITY MEASURES RATHER THAN REACTIVE ONES. ***ANDY MACKAY - MARKETING DIRECTOR EMEA, GENETEC"***

Interview with Quintin Roberts – Regional Sales Manager Africa, Genetec

How has Intersec 2025 compared to previous years in terms of engagement, and what key innovations is Genetec showcasing this year?

Intersec 2025 has seen an incredible first day, with strong footfall and increased engagement from industry professionals across the Middle East, Africa, and even Asia-Pacific. There is a clear demand for knowledge on evolving security technologies, and the event continues to attract a global audience.

This year, Unification remains a top priority for Genetec. We have introduced several new hardware integrations through our technology partners, such as Axis Communications, and expanded the new 4 and 8 door Axis Powered by Genetec network door controllers. Additionally, we have launched Security Center 5.13, which focuses on automation to simplify system configuration and enhance user experience. These innovations align with the industry's shift toward smarter, more efficient security solution

How does Genetec select and support its channel partners in the Middle East and Africa?

Genetec follows a focused partner strategy rather than prioritizing volume. We do not believe that having more partners necessarily translates to more business. Instead, we carefully select partners whose expertise aligns with our solutions, ensuring they can effectively implement and support our products.

In Africa, we operate a mixed model, with partners spread across East, West, Central, and North Africa. The demand for training and access to our brand is increasing, and we continuously evaluate the market to onboard partners who meet our high standards. Through our dedicated training division, we provide tailored training for both integrators and end-users, ensuring they maximize the potential of their investments in our technology.

How is the UAE shaping digital transformation in security, and how does it influence Genetec's strategy?

The UAE is a global leader in digital transformation, consistently setting new benchmarks in technology and security. The country's ability to rapidly implement policies and drive technological advancements serves as a model for

other regions, including Africa.

From a Genetec perspective, we closely observe the UAE's progress and innovation to align our strategies. The region's commitment to smart cities, AI-driven security, and cybersecurity compliance creates a strong market for our solutions. The UAE's digital-first approach provides valuable insights into how we expand and refine our offerings globally.

How has Genetec's business in Africa evolved, and what has been the impact of 2024 on its growth?

Genetec has experienced phenomenal growth in Africa, achieving record-breaking years consecutively. The demand for unified security solutions has fueled expansion into new regions, increasing our market share and staff presence.

In 2024, we saw strong business performance across multiple African markets, demonstrating the impact of our differentiated unified security offering. Our solutions continue to drive operational efficiency for customers, and with a healthy pipeline for 2025, we aim to replicate this success in the coming years.

How does Genetec empower its channel partners and customers with the necessary skills and training?

Genetec has a dedicated training division that provides in-depth training for both certified channel partners and end-users. Our training programs include:

- Operator Training (various levels)
- Custom Training Modules tailored to specific needs
- In-person, virtual, and self-paced blended certification programs
- Professional Services for technical account management and ongoing support

Quintin Roberts – Regional Sales Manager Africa, Genetec

The goal is to bridge the gap between technology and users, ensuring customers fully utilize the capabilities of their security solutions rather than just a fraction of them.

How is Genetec integrating AI and automation into its security solutions?

Genetec has several AI-driven capabilities within Security Center, including:

- Mission Control, which automates and digitizes standard operating procedures, reducing manual processes.
- AI-powered data correlation through integrations with our technology partners, allowing for smarter insights.
- Customizable dashboards that provide real-time operational intelligence across industries.

By leveraging AI, we enhance operational efficiency, enabling businesses to automate security workflows, analyze large datasets, and improve decision-making.

How do Genetec's solutions help businesses improve operational efficiency beyond security?

While Security Center was initially designed for security and safety, it has evolved to support industrial IoT integration, allowing businesses to extract insights from non-security devices such as:

- Building management systems
- IoT sensors
- Retail analytics tools

By consolidating data from multiple sources, businesses can create custom dashboards for different departments, including security teams, facility management, and marketing. For example, in retail, heat maps and transaction analysis can help measure marketing campaign effectiveness.

Ultimately, our solutions help organizations maximize asset utilization, enhance security operations, and leverage business intelligence to drive greater efficiency across all functions.

> **"THROUGH OUR DEDICATED TRAINING DIVISION, WE PROVIDE TAILORED TRAINING FOR BOTH INTEGRATORS AND END-USERS, ENSURING THEY MAXIMIZE THE POTENTIAL OF THEIR INVESTMENTS IN OUR TECHNOLOGY**
>
> ***QUINTIN ROBERTS – REGIONAL SALES MANAGER AFRICA, GENETEC"***

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**

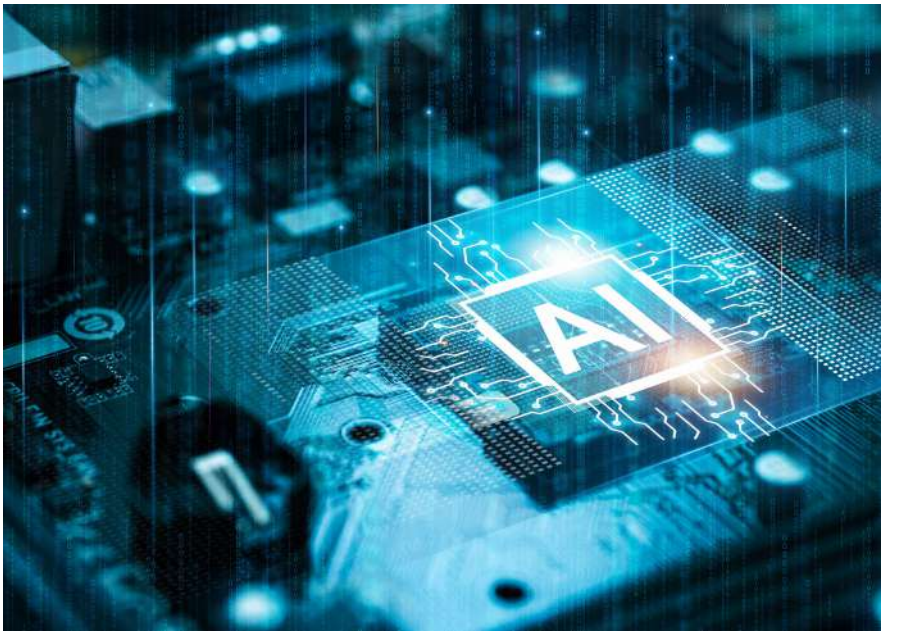
FORTINET

WESTERN DIGITAL LEADS FUTURE OF STORAGE FOR AI, SMART CITIES, AND MORE

MOHAMMED OWAIS, SALES DIRECTOR, MIDDLE EAST AT WESTERN DIGITAL, SHARES INSIGHTS ON THE EVOLVING DATA STORAGE LANDSCAPE, THE IMPACT OF AI, AND THE UAE'S ROLE AS A DIGITAL TRANSFORMATION HUB.

Data has become the lifeblood of innovation, powering everything from Artificial Intelligence (AI) to smart cities. At the forefront of this evolution is Western Digital, a company that has been instrumental in advancing storage technologies to meet the ever-growing demand for high-capacity and high-performance solutions.

At Intersec 2024, Mohammed Owais spoke to Sandhya D'Mello, Technology Editor, CPI Media Group to discuss the company's latest innovations, the role of AI and cloud computing in shaping the future of data storage, and how the UAE is positioning itself as a global digital leader.



How does Intersec 2024 compare to previous years, and how has the event benefited your company?

Intersec 2024 has been an incredibly important event for us. It provides a platform to engage with partners across the Middle East, gain insights into the latest technology trends, and explore innovations in surveillance, AI, and cloud storage.

One of the biggest advantages of being at Intersec is that it allows us to stay ahead of market trends and understand the evolving needs of the industry. Surveillance, DVR (Digital Video Recorders), NVR (Network Video Recorders), and other ecosystem players are key areas where we see advancements, and this event gives us a chance to strengthen our relationships with partners, both new and existing.

We've been participating in Intersec since its inception, and our investment in the event has grown significantly over the years, demonstrating our commitment to the region.

What key innovations Western Digital showcased at Intersec 2024?

This year, our stand is designed to be minimalistic and futuristic, focusing on delivering a clear, immersive experience rather than cluttering the space with excessive elements.

One of the highlights is our AR demo of the JBOD solution, where customers can interactively explore its components, turn it around, and understand how Western Digital's patented technologies are integrated into the system.

Additionally, we have introduced our 26TB Purple Pro and 32TB Ultrastar, marking a major step in high-capacity storage solutions. These products cater to growing demands in surveillance, AI, and enterprise storage, offering enhanced reliability and scalability.

When will these new storage solutions be commercially available?

The 26TB and 32TB drives are currently undergoing qualification in the region, meaning they are being tested with various customers before commercial availability. Since these are specialized, high-capacity storage solutions, the qualification process takes time. We anticipate they will be available in the market in the coming weeks.

With rapid technological advancements, how should businesses approach data storage investments?

The key is to strike a balance between innovation and practical business needs. Many companies rush to adopt new technologies without considering their long-term sustainability or compatibility with existing infrastructure.

From Western Digital's perspective, storage is the backbone of digital transformation. Whether it's AI, smart cities, or IoT, hard drives remain a critical component in six key stages of data

"HAVING SPENT 27 YEARS IN THE UAE, I'VE WITNESSED FIRSTHAND HOW THE COUNTRY HAS EVOLVED INTO A DIGITAL POWERHOUSE. THE UAE IS NOT JUST ADOPTING NEW TECHNOLOGIES—IT'S SETTING GLOBAL BENCHMARKS IN AI, SMART CITIES, AND DIGITAL GOVERNANCE "

processing, from storage to rendering and analytics.

Businesses should ensure their storage solutions align with their operational needs, optimizing for scalability, security, and efficiency rather than just chasing trends.

In the age of cloud computing, is physical storage still relevant?
Absolutely. Many assume that cloud computing eliminates the need for physical storage, but that's a misconception. Cloud infrastructure relies on physical storage, particularly hard drives, at hyperscale data centers, enterprise environments, and local storage solutions.

The Total Cost of Ownership (TCO) is also a key factor. Hard drives offer superior cost-efficiency per gigabyte compared to other storage technologies, making them a preferred choice for long-term data retention and security.

How is AI, particularly Generative AI, shaping the future of data storage?
AI-driven applications, especially Generative AI, require unprecedented storage capacities. Whether it's data training, processing, or analytics, AI depends heavily on fast, scalable, and reliable storage solutions.

At Western Digital, we like to say, "Data is the new oil, and we have the barrels." As AI adoption grows, we anticipate an increased demand for high-capacity, high-performance storage solutions, making data management and optimization more crucial than ever.

The UAE is seen as a leader in digital transformation. How do you view its growth in the tech sector?
Having spent 27 years in the UAE, I've witnessed firsthand how the country has evolved into a digital powerhouse. The UAE is not just adopting new technologies—it's setting global benchmarks in AI, smart cities, and digital governance.

The government's investment in futuristic technologies makes the UAE the epicenter of digital evolution in the MENA region. Whether it's AI-driven infrastructure, blockchain adoption, or cloud security, the UAE is at the forefront, often ahead of many developed nations.

How was 2024 for Western Digital, and what are your key focus areas for 2025?
2024 has been a phenomenal year for us, with increasing demand for storage solutions across industries. Whether it's enterprise data centers, surveillance, healthcare, or AI applications, the need for efficient, scalable storage has never been greater.

For 2025, our top three focus areas in the Middle East will be:

1. Strengthening alliances with ecosystem partners – Building stronger collaborations within the data storage, cloud, and AI ecosystems.
2. Training and education – Ensuring our customers and partners understand evolving storage technologies and how they can benefit from them.
3. Expanding our regional footprint – Growing our presence and influence across the Middle East.

The data storage industry is evolving rapidly, and Western Digital remains committed to driving innovation in AI, cloud computing, and high-capacity storage solutions. As the UAE continues its journey toward becoming a global digital hub, storage solutions will play a pivotal role in shaping the future of technology and digital transformation.

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 دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

OFFICIALLY SUPPORTED BY
وزارة الداخلية
MINISTRY OF INTERIOR
شرطة دبي
DUBAI POLICE

GUINNESS WORLD RECORDS
RECORD HOLDER

MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT

SCAN HERE

ENQUIRE FOR 2025!

OFFICIAL DISTRIBUTION PARTNER
SPIRE

LEAD STRATEGIC PARTNER
HUAWEI

DIGITAL TRANSFORMATION PARTNER
du BUSINESS

STRATEGIC PARTNERS
Microsoft
etisalat and beyond

PLATINUM SPONSORS
PENTERA
cisco
aws

GOLD SPONSORS
CLOUDFLARE
emt
sg
kaspersky
MENLO SECURITY
NOKIA
OPTIMAS
Qualys.
SANS | GIAC CERTIFICATIONS
tenable

SILVER SPONSOR
Recorded Future

CONTACT US

gisec@dwtc.com
+971 4 308 6469
cyber.gisec.ae
#gisecglobal

SECURE DOMAINS BRINGS CUTTING-EDGE DNS PROTECTION TO MENA REGION

DUBAI'S HOMEGROWN CYBERSECURITY STARTUP LAUNCHES THE REGION'S FIRST CLOUD-BASED DNS FIREWALL SERVICE, STRENGTHENING DIGITAL DEFENSE FOR BUSINESSES ACROSS MENA.

Dubai-resident, Wissam Saadeddine is on a mission to offer a secure digital space through his home-grown, recently launched, Secure Domains. The self-funded venture — which is open to raise funds in mid-2025 — was founded with the mission to deliver unparalleled cloud-based cybersecurity services. It is the first company in the GCC and Africa to offer cloud-based DNS firewall services and security through its flagship SaaS product, 'DNS Armor'.

The product DNS Armor stands out for its top-tier security features and user-friendly interface, allowing it to be tailored precisely to meet the unique needs of each client. Its flexible implementation and highly customizable design ensure that it can be applied and scaled efficiently according to specific requirements.

Wissam Saadeddine, Co-Founder of Secure Domains spoke to Sandhya D'Mello, Technology Editor of CPI Media Group about what compelled him to take the entrepreneurial journey and offer the best to the Middle East region with Dubai playing a key role in nurturing his ambition to protect businesses from cyber threats.

Can you discuss the importance of DNS in digital security based on your experience?

During my previous work stint, which spanned nearly a decade, I gained profound insights into the critical role of DNS (Domain Name System) in securing digital infrastructures. We always emphasize DNS as the foundational layer of defense in any security architecture—be it for organizations or individuals aiming to safeguard their business and minimize risks.

Throughout those years, we observed a growing awareness of DNS's importance, though it was initially overlooked by many in their security strategies. This shift in perspective became crucial as businesses increasingly moved towards digital transformation and cloud services. Essentially, every online activity begins with a DNS query, whether it's checking emails or accessing applications like WhatsApp. This initial transaction, the DNS query, seeks to locate and connect with the desired online destination.

Recognizing the potential of DNS to act as a security filter, it can significantly enhance protection by screening out malicious sites right from the start, thus mitigating risks early in the cyber kill chain. This realization led me to appreciate DNS not just as a utility but as a potent security tool, which, however, hadn't received adequate attention for its integration into broader security frameworks.

My previous workplaces continued to emphasize the importance of DNS, particularly in distributed and

borderless infrastructures. However, the focus on DNS as a primary security gateway remained inadequate. This led to the creation of a new platform, developed in collaboration with my colleague Mohammad and other developers, aimed at utilizing the full potential of DNS.

We envisioned a platform that was not only robust and compliant with data sovereignty and local regulations but also MSP-ready, supporting multi-tenancy to cater to service providers. This comprehensive approach has enabled us to offer a customized DNS service that meets the specific needs of diverse organizational environments, thereby reinforcing DNS as the cornerstone of digital security architecture.

DNS is often overlooked as a critical security layer. What are the biggest challenges in raising awareness about its importance, and how does your platform address these gaps?

Organizations must prioritize DNS as the first layer of defense in their cybersecurity architecture. Everything we do online, from checking emails to using apps, starts with a DNS query. If we empower DNS with security features, it can serve as a powerful filter to block threats at the earliest stage of the cyber kill chain.

Over the period of time, I realized that DNS security still wasn't getting enough attention as the first security gateway and that's when I started thinking—why not create our own platform? Together with Mohammad (one of our key developers), we saw a major gap in the market: Limited awareness about DNS security's role as the first layer of defense; Compliance challenges—existing DNS services from global providers did not fully comply with local data sovereignty and residency regulations set by governments and central banks; and MSP readiness—we needed a multi-tenant, MSP-ready platform that service providers could offer as a fully managed solution for their customers.

With these three key pillars in mind, we built our own cloud-based DNS security platform, hosted locally to ensure regulatory compliance while providing robust, first-line defense against cyber threats. Now, we are actively marketing it across the region, ensuring that organizations have a secure, compliant, and scalable DNS security solution.

What were the driving factors behind the decision to build a localized solution instead of relying on multinational solutions?

The idea started about a year and a half ago. We believed in the concept and the service we wanted to deliver, but we needed to make it our own and market-ready. Instead of relying on multinational solutions that are shipped to our region, we decided to build a solution locally—tailored for this market, compliant with regulations, and fulfilling the region's needs.

When you launched DNS Armor, what was the initial response? Was there resistance to your solution?

We just launched DNS Armor recently so we don't have an extensive track record yet. However, we did a pre-launch phase, engaging with customers and partners, and the response was better than expected. Businesses are keen to adopt a UAE-based vendor rather than relying on global providers, there is a strong support for a regionally built security platform compliant with local regulations.

What are your growth plans for the MENA region?

The platform is already up and running across multiple countries. Our cloud infrastructure is operational in the UAE, Qatar, and other parts of the region. For now, our focus is on expanding in the UAE, Qatar, and Saudi Arabia, while also partnering with MSPs in Kuwait and Egypt. Our go-to-market strategy is channel-driven, working through partners to grow across the broader MENA region.

Looking beyond DNS Armor, what innovations do you plan for 2025?

Our roadmap is built on three key phases:

1. Enhancing DNS security – Leveraging AI and threat intelligence to detect sophisticated cyber threats.
2. Expanding to DDI (DNS, DHCP, and IP Address Management) – Strengthening network security.
3. Developing a Secure Web Gateway – To protect all internet traffic, beyond just DNS.

Eventually, we aim to build a full-fledged SASE (Secure Access Service Edge) platform, but we are starting by establishing a robust security foundation first.

How does DNS Armor address cybersecurity threats in the region?

A major cybersecurity gap is that data can leak through DNS traffic, bypassing even the most advanced security solutions. Attackers can stealthily extract data using zero-day domains—domains with no history of being malicious—making them difficult to detect.

DNS Armor prevents this by:

- Using AI-driven threat intelligence with 30 million+ malicious domain indicators (IOCs).
- Detecting and blocking malicious DNS traffic before it reaches an organization's network.
- Preventing data exfiltration by monitoring DNS queries in real-time.

This solution protects users anywhere, whether they are in an office or working remotely, ensuring DNS is the first line of defense against cyber threats.

LEAP

09-12 FEBRUARY 2025
RIYADH, SAUDI ARABIA

INTO NEW WORLDS

680+ start-ups

1,000 speakers

1,800+ global tech brands

170,000+ global attendees

Step into what's next. Secure your ticket now

www.onegiantleap.com

Co-organised by:

وزارة الاتصالات وتقنية المعلومات
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES

tahaluf
an informa company
تحالف

SANS CYBER ACADEMIES: BUILDING CYBER WORKFORCE OF TOMORROW

EMPOWERING CYBERSECURITY DEFENDERS WITH TAILORED TRAINING, GLOBAL CERTIFICATIONS, AND INCLUSIVE OPPORTUNITIES

In today's digital age, cyber threats are evolving at an unprecedented pace, targeting critical infrastructure, sensitive data, and economic stability. The global cybersecurity skills gap continues to widen, leaving organizations vulnerable to attacks that can disrupt operations, compromise safety, and cause significant financial and reputational damage. Cybersecurity education is no longer optional—it's a necessity.

By equipping professionals with the skills to defend against sophisticated threats, we can safeguard industries, protect communities, and foster innovation. SANS Cyber Academies are at the forefront of this mission, delivering tailored, hands-on training that addresses regional and industry-specific challenges while building a diverse and resilient cybersecurity workforce.

SANS Cyber Academies are revolutionizing cybersecurity education by delivering fast-tracked, hands-on training programs designed to address the global skills gap. With a focus on regional and industry-specific needs, SANS equips professionals with practical skills and globally recognized certifications, empowering them to tackle evolving cyber threats.

Ned Baltagi, Managing Director, Middle East, Turkey and Africa, at SANS Institute spoke to Sandhya D'Mello, Technology Editor, CPI Media Group about safeguarding critical infrastructure in the Gulf to fostering diversity and inclusion in the cybersecurity workforce, SANS Cyber Academies are building a resilient, skilled, and diverse community of defenders ready to secure the future.

"SANS CYBER ACADEMIES DON'T JUST TRAIN INDIVIDUALS—THEY BUILD RESILIENT, DIVERSE, AND HIGHLY SKILLED COMMUNITIES READY TO TACKLE THE WORLD'S MOST PRESSING CYBERSECURITY CHALLENGES"

Can you elaborate on the impact of SANS Cyber Academies in the Middle East, particularly in how they are addressing the cybersecurity skills gap across critical sectors?

At SANS Institute, we are tackling the pressing cybersecurity skills gap through the SANS Cyber Academy, a fast-tracked training program designed to deliver impactful results. Participants gain practical, hands-on skills taught by world-class SANS Instructors, enabling them to make an immediate impact in the real world. What makes the SANS Cyber Academy unique is its tailored approach. In the Middle East, we work closely with local government organizations and industry leaders to design programs that target specific industries and address their cybersecurity challenges. This ensures our graduates are not only highly skilled but also well-equipped to tackle the region's most pressing security needs.

Consider the Gulf region, where critical infrastructure underpins economic stability and public safety. Cybersecurity

upskilling is essential, and defenders require specialized training to tackle threats effectively, all while maintaining a focus on safety. At SANS, our academies are designed to adapt to organizational and regional needs, ensuring the training remains relevant and impactful.

For example, we recently delivered two Cyber Academies in Kuwait, equipping participants with the skills and strategies to combat evolving cyber threats in a high-stakes industry. Programs like these exemplify our commitment to providing targeted, results-driven training that empowers teams to excel in their specific environments. Every team member, from technical staff to leadership, must develop the expertise required to address cybersecurity challenges across all business sectors. Whether it's safeguarding critical infrastructure in ICS/OT environments or protecting sensitive data in the financial sector, tailored expertise is essential to meet the unique demands of each industry.

What are the most pressing cyber threats currently impacting the Gulf region's infrastructure, and how is SANS working to mitigate these threats through its training programs?

The Gulf region's critical infrastructure faces increasingly sophisticated cyber threats, with adversaries exploiting both IT and ICS environments. Sectors like Oil and Gas and Energy are particularly targeted, as attackers aim to disrupt operations, compromise safety, and even cause environmental harm. Incidents like TRISIS/TRITON and ransomware attacks, including EKANS, can cause catastrophic physical damage, operational shutdowns, and severe financial losses, jeopardizing lives and environmental safety. Specialized cybersecurity training, therefore, is essential to combat threats and high-stakes risks in industrial environments.

SANS Institute addresses these challenges through its ICS curricula and training programs, equipping professionals with the required skills to protect these critical systems. Courses like ICS410: ICS/SCADA Security Essentials lay a strong foundation for securing industrial environments, while ICS515: ICS Visibility, Detection, and Response teaches teams advanced threat detection and incident response, using hands-on labs with real hardware.

For leaders, ICS418: ICS Security Essentials for Leaders focuses on aligning cybersecurity strategies with business objectives, helping them manage industrial cyber risks effectively. Meanwhile, courses like ICS456 and ICS612 dive deeper into standards compliance and advanced technical defenses, providing practical, real-world expertise.

How do SANS Cyber Academies adapt their curriculum to meet the specific needs of different global and regional markets, and can you provide examples of how these programs are customized to foster diversity in cybersecurity professions?

We offer a range of Cyber Academies tailored to diverse pathways, empowering individuals globally with specialized, accessible training that builds foundational cybersecurity skills and prepares them for impactful careers.

For instance, in partnership with Tamkeen, the Bahrain Cyber Reskilling Program provided intensive eight-week training for Bahraini nationals aged 18 and above, culminating in three GIAC certifications. This initiative directly addressed the local skills gap and equipped participants with globally recognized credentials to advance their cybersecurity careers.

Breaking gender barriers, our Women's Pathway, fosters inclusion and leadership for women and underrepresented genders in cybersecurity. Programs like the Women's Cyber Academy and Secure Diversity Leadership Academy, in collaboration with organizations such as WiCyS, offer scholarships

and certifications to help women and underrepresented genders lead in cybersecurity.

Our Veterans Pathway supports US military veterans and spouses transitioning into cybersecurity with comprehensive and immersive training that covers the latest technologies and techniques used in the field building on existing military expertise to further cybersecurity careers.

With our Diversity Pathway, programs like Cyversity SANS Diversity Academy, funded by Google and Palo Alto Networks, and Jumpstart into Cyber, backed by NSF, empower underrepresented groups with no-cost training, gamified learning, and certification opportunities.

Our goal is to create a more inclusive and diverse cybersecurity landscape through these academies, equipping individuals with the knowledge, skills, and certifications needed to build

successful careers. At the same time, we address critical industry challenges by fostering a dynamic and resilient workforce prepared to tackle the evolving cybersecurity threat landscape.

In what ways do the SANS Cyber Academies' programs contribute to upskilling and reskilling, particularly in the context of the rapidly evolving cyber threat landscape? What opportunities does this create for professionals seeking to enter or advance in the cybersecurity field?

Not only do the SANS Cyber Academies address the skills gap in the specific sector it is targeting, but they also contribute to the growth of local cyber talent in organizations. We are constantly recruiting individuals with curiosity and a drive to learn for our SANS Cyber Academies, as these programs encourage continuous development. These academies provide an accessible opportunity for individuals who may have not recognized their aptitude for cybersecurity - or lacked the means to explore the field - to discover their potential and develop their skills. Organizations can amplify this by partnering with us or allocating resources for ongoing education during onboarding. Investing in training not only strengthens defenses against emerging threats but also enhances employee retention by fueling their passion for learning and staying current, creating a workforce that is both skilled and motivated to contribute effectively.

Moreover, the SANS Cyber Academies offer a faster, more impactful alternative to standalone training, equipping individuals with certifications like GIAC in weeks rather than months, while maintaining exceptional success rates. Beyond training, they build a community of like-minded, skilled professionals and benefit the broader industry.

How does the education provided by SANS Cyber Academies benefit the wider community and nation, and what impact does this have on the growth and resilience of the cybersecurity sector?

Addressing the growing cybersecurity threats requires a workforce that is both skilled and diverse. SANS Cyber Academies actively work to bridge this gap by equipping individuals from varied backgrounds with advanced cybersecurity knowledge and practical skills. Our academies represent more than just a learning opportunity, they provide a pathway for participants to contribute innovative ideas and solutions to the cybersecurity sector. By welcoming talent that has historically been underrepresented in the industry, the academies help drive creativity, enhance leadership opportunities, and strengthen the overall resilience and growth of the cybersecurity field at a national and global level.

The education provided by SANS Cyber Academies strengthens national security, bridges the cybersecurity skills gap, and empowers individuals with industry-recognized certifications. For instance, the program in Kuwait saw students consistently achieving high marks in their GIAC certifications, demonstrating the effectiveness of the training and their readiness to excel in the field. Participants also benefited from the support of a robust cybersecurity community, fostering collaboration and shared learning. Beyond individual achievements, SANS contributed to the wider community through security events and resource sharing, promoting broader awareness and resilience, and the program delivered highly trained employees who are better equipped to safeguard critical assets, mitigate risks, and support organizational cybersecurity strategies. These outcomes collectively enhance community resilience, drive innovation, and support economic growth while building a more secure and inclusive cybersecurity sector.

DATA PRIVACY DAY 2025 CHAMPIONS GLOBAL EFFORTS TO PROTECT PERSONAL DATA

EMPOWERING INDIVIDUALS, BUSINESSES, AND GOVERNMENTS TO SECURE DATA, FOSTER TRANSPARENCY, AND BUILD A RESILIENT DIGITAL FUTURE.

Data protection is critical because it safeguards sensitive personal and organizational information from unauthorized access, theft, and misuse. In today's digital age, data is an asset that fuels innovation and decision-making, but it is also a prime target for cybercriminals. Breaches can lead to financial losses, identity theft, reputational damage, and legal consequences.

For businesses, failing to protect data erodes customer trust and loyalty. With the rise of AI, cloud computing, and hybrid work environments, the complexity of data management has increased, making robust security measures essential. Prioritizing data protection ensures privacy, compliance with regulations, and a secure digital ecosystem for all.

Data Privacy Day, established in 2007 by the Council of Europe, marks January 28 as a day to commemorate the signing

of Convention 108 in 1981—the first legally binding international treaty on data protection. Over the years, it has evolved into a global observance, recognized not only in Europe but also in the US, Canada, and other regions.

The day's primary objective is to spotlight the critical importance of safeguarding personal data and privacy rights in an era defined by rapid technological advancements and increasing cyber threats. It aims to educate individuals, businesses, and governments about best practices for securing sensitive information, complying with privacy regulations, and fostering trust and transparency in data management.

With cyberattacks and data breaches on the rise, Data Privacy Day serves as a wake-up call for individuals to take ownership of their digital footprints and for organizations to prioritize robust data protection measures. By promoting proactive strategies such as encryption, access controls, and regulatory compliance, the day underscores the shared responsibility of securing the digital ecosystem.

For a security professional, Data Privacy Day is more than a symbolic reminder—it's a rallying point for advancing privacy-conscious innovations and embedding security into every layer of the digital infrastructure.

Maher Jadallah, Vice-President, Middle East and North Africa, Tenable

Data is the lifeblood that decisions are made on - it fuels innovation in the cloud, but the volume and complexity in hybrid and multi-cloud environments makes it difficult to secure. You can't have privacy without security!

Protecting data in public cloud environments starts with answering three seemingly simple security questions:

What type of data do I have in the cloud? How is it classified? Is it sensitive?

Where is my sensitive data in the cloud? Who has access?

What are the risks to my cloud data?

"Security teams need a comprehensive view of their cloud data and the risks associated with it. This Data Privacy Day, every organisation must take action to protect the data it relies upon to function and that it's trusted to protect, wherever it resides."

Meriam ElOuazzani, Senior Regional Director META, SentinelOne

Data Privacy is the foundation of trust in our AI-driven world. As generative AI reshapes industries, the responsible handling of personal data becomes more critical than ever. Organizations must embed privacy-by-design principles into every AI implementation, ensuring data is protected from creation to consumption. With AI's growing capabilities, safeguarding against misuse, bias, and unauthorized access is essential to maintain trust.

"On this Data Privacy Day, let's prioritize transparency, secure AI practices, and empower individuals with control over their data. Together, we can harness the power of generative AI responsibly, building a future where innovation and privacy coexist seamlessly."

Sreedharan KS, Director of Compliance, ManageEngine, Zoho Corporation

As we mark Data Privacy Day in 2025, it highlights the need and attention on why safeguarding data is an essential need going forward for businesses and individuals concerned. With the digital landscape bombarded with cybersecurity issues, especially with the growing challenges and opportunities brought forth by AI and ML capabilities, industries such as Healthcare, Telecom, BFSI have all reshaped in how data is collected, stored and used. With the expanding possibilities with AI and ML, it has also put boundaries on how data can be collected and analyzed as well, leading to compliance violations for businesses if this aspect is left unchecked.

Data privacy and protecting an individual's data should not be viewed as a restriction but an active necessity to safeguard data from exploitation, leading to better trust and bonding between individuals and businesses.

"By emphasizing privacy regulations, companies can use it as a competitive advantage to foster trust and maintain long-term fruitful relationships with customers, thereby driving responsible yet sustainable growth in the AI-domained world we live in."

Ranjith Kaippada, Managing Director of Cloud Box Technologies

As we mark Data Privacy Day on January 28, it is crucial to emphasize the importance of safeguarding personal and professional information in today's digital world. Data is no longer just bits and bytes; it has the potential to cause significant harm to users, exposing them to countless risks such as financial fraud, identity theft, phishing attacks, irreparable reputation damage, and more.

"For businesses, implementing strong data privacy practices is essential for customer loyalty. This Data Privacy Day, take a pledge to protect your data. It isn't just about meeting legal obligations but a shared responsibility to build a secure and trustworthy digital ecosystem."

Chester Wisniewski, director, field CTO, Sophos

It's 2025 and we still report on data breaches every single day, so making an effort to protect our information is as important as ever. While encryption on the web is nearly ubiquitous, many of us still rely on email for sensitive communications, which it is important to move on from.

"Time and again we see SMS and email messages hacked, stolen, and breached and we must all move toward all sensitive communications being on end-to-end encrypted platforms like Signal."

HALCYON NAMES RAAS GROUPS TO WATCH FOR IN 2025

LEADING ANTI-RANSOMWARE PLATFORM ALSO REVEAL COMMON TACTICS, TECHNIQUES, AND PROCEDURES USED BY ATTACKERS

The ransomware landscape shifts quickly, as highlighted by the continued rise and fall of various Ransomware-as-a-Service (RaaS) groups. These groups offer tools and infrastructure that enable affiliates to attack. While their tactics are innovative and aggressive, they are inherently unstable, as they experience source code leaks and internal and external disputes.

Halcyon, the first dedicated anti-ransomware platform that uses advanced prevention tools, automated recovery, and enhanced security integrations, has unveiled its list of top RaaS groups and the Tactics, Techniques, and Procedures (TTPs) to watch for in 2025. This is in a bid to help various organizations boost their cybersecurity defenses, especially against attacks carried out by ransomware operators.

Top established RaaS groups

The past years saw the decline of major players like LockBit and BlackCat/ALPHV. But along with it is the emergence of RaaS groups that have swiftly established themselves as huge threats.

For 2025, Halcyon identified established RaaS groups to watch for.

- Play is one of the most active and innovative groups in the RaaS space. The group operates with tactics similar to the now-defunct ransomware strains, Hive and Nokoyawa.
- RansomHub has carried out high-impact attacks since its emergence in early 2024. It sets itself apart from other groups by offering affiliates up to 90% of ransom payments.
- 8Base deploys sophisticated tactics, including double extortion and advanced evasion techniques. It's believed to be tied to experienced RaaS operators like RansomHouse and the Babuk ransomware builder.
- Qilin, previously known as Agenda, is a RaaS operation that targets both Windows and Linux systems. It's written in Golang and Rust, the latter of which boasts superior security and cross-platform capabilities.
- BlackSuit is a private ransomware group that targets Windows and Linux systems. It shares similarities with Royal ransomware in terms of code structure and encryption methodology.
- Hunters International only emerged in October 2023 but by 2024, it has already conducted over 130 attacks. Leveraging the codebase from Hive, the group targets industries like healthcare, finance, and manufacturing.

Top emerging RaaS groups

Apart from established RaaS groups, Halcyon also named notable emerging groups to keep on the cyber radar.

- Sarcoma is a group that gained notoriety for its aggressive tactics and data breaches. Instead of listing ransom amounts, it uses data leaks to pressure victims into compliance.

- Fog ransomware has garnered attention with its swift file encryption and ransom demands in Bitcoin. It has since expanded, carrying out more lucrative and high-profile attacks.
- Originally a hacktivist group linked with the Anonymous movement, KillSec launched its RaaS platform in June last year. It earns a 12% commission on each payment.
- Meow Ransomware was first identified in 2022 and re-emerged in 2024. Linked to the Conti v2 variant, it targets U.S. industries handling sensitive data, including healthcare and medical research.

Top TTPs for RaaS Operations

This 2025, ransomware groups are expected to continue using sophisticated tactics, techniques, and procedures (TTPs) to enhance their attacks and evade detection.

Social engineering remains a top infection vector. Other common infection vectors for RaaS operators include brute forcing and leveraging stolen RDP and VPN credentials. Halcyon also foresees unpatched vulnerabilities being heavily exploited.

In 2025, more Linux systems could be targeted by ransomware groups, leveraging these systems' "always on, always available" nature to establish command and control.

Ransomware operators also increasingly use Living-off-the-Land (LotL) techniques to avoid detection. Along with this, these groups develop custom cross-platform payloads and data exfiltration tooling, making data theft a standard in nearly every major operation.

Attackers bypass modern security defenses, such as EPP, EDR, and XDR tools, through advanced techniques like unhooking, blinding, and the deletion of shadow copies or cloud backups.

Additionally, more advanced TTPs, often seen in APT-style operations, are becoming prevalent. These include exploiting zero-day vulnerabilities, employing DLL side-loading, and leveraging payloads written in languages like Rust and Go.

While many ransomware groups still target low-hanging fruit, such as vulnerable applications or poorly defended systems, advanced operators also focus on certain sectors — with high-value sectors such as healthcare, critical infrastructure, manufacturing, and online commerce being prime targets. Additionally, industries with limited cybersecurity resources, such as the education sector and state or local governments, remain vulnerable.

As the ransomware landscape continues to see such shifts, Halcyon remains committed to providing advanced solutions alongside insightful reports. Quarterly, it publishes its Ransomware Malicious Quartile report. This report ranks ransomware groups according to key factors such as attack volume, sophistication, and impact.

RANSOMWARE SPOTLIGHT - HOW THREAT ACTORS USE C2 AND DATA EXFILTRATION AS PART OF DOUBLE EXTORTION

Krupa Srivatsan, Senior Director, Cybersecurity Product Marketing at Infoblox

Ransomware attacks have become a significant concern for organizations worldwide, with the frequency and success of these attacks continuing to rise. Ransomware attacks can have devastating consequences for businesses, including costly downtime, data theft, and reputational damage. The average downtime and recovery time after a ransomware attack is 22 days, with a conservative estimate of the cost of downtime being $43.2 million.

Typically, in ransomware attacks, cybercriminals gain access to a company's data and use encryption to prevent users from accessing that data until a ransom is paid. As these types of attacks became widespread, organizations started to have robust backups so that they could recover their data in case of a ransomware attack and would not have to pay the ransom. To increase the pressure on victims to pay the ransom, cybercriminals then started to resort to double extortion ransomware, where the attackers not only encrypt sensitive data but also steal the data and threaten to publish it on the dark web if the ransom is not paid. Preventing the leakage of sensitive information is critical for companies as such data leaks can result in fines, loss of brand reputation, and lost customers.

Use of DNS by Ransomware for Command and Control (C2) Communications

Once ransomware has infiltrated a company's network and begins executing, it utilizes Command and Control (C2) communications to download the encryption key to the end host and encrypt the files. This C2 happens over DNS. DNS C2 is a technique used by cybercriminals to communicate with malware that has infected a target system. Also called beaconing, the malware periodically sends DNS queries to the attacker's server to check for new commands. This communication is crucial for controlling the malware and executing malicious activities.

Cybercriminals use DNS for C2 because:

- It is a ubiquitous and essential service in network communications. By embedding commands within DNS

queries and responses, attackers can communicate with malware without raising suspicion.

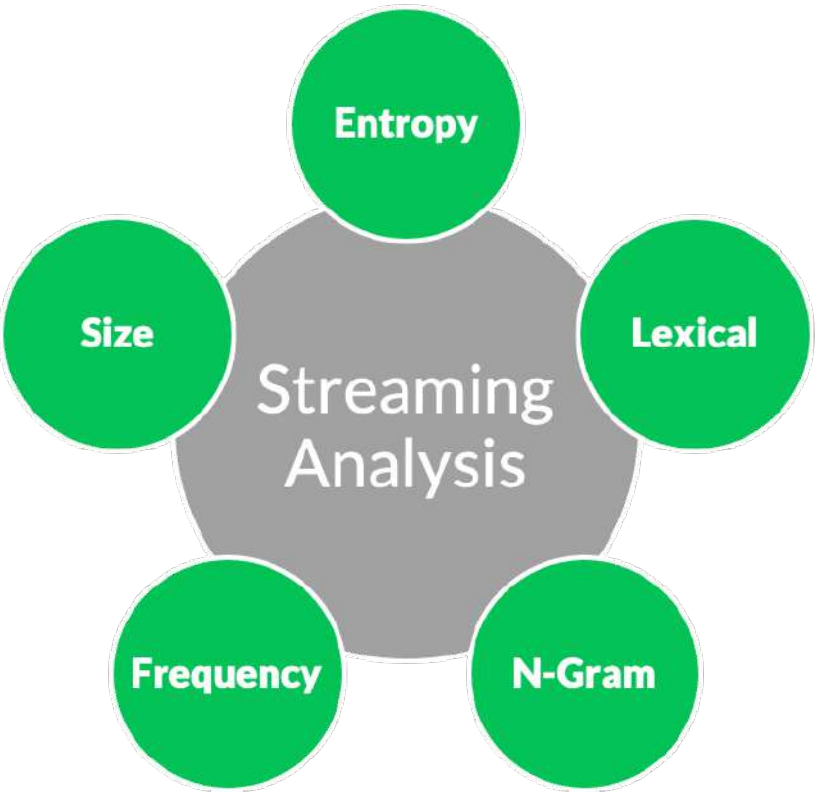
- It provides a level of stealth. Since DNS traffic is usually allowed through firewalls and other security devices, it can be used to hide malicious activities. Attackers can encode commands in DNS queries and responses, making it difficult for security tools to detect and block these communications

Use of DNS by Ransomware for Data Exfiltration

In addition to using DNS to relay commands/data out of the organization, ransomware attacks, especially ones that are double extortion, as defined at the beginning of this blog, get hold of sensitive data, such as credit card data, and send this data out in DNS queries. These queries are sent to a malicious DNS server controlled by the attacker. The server decodes the data from the queries and stores it. Data exfiltration over DNS is a sophisticated technique that allows attackers to covertly transfer sensitive data out of an organization by leveraging the DNS protocol. By embedding data in DNS queries, or in other words creating a tunnel over DNS to transfer data, attackers can bypass traditional data loss prevention (DLP) tools that might block other avenues of data theft.

Proactive Blocking of Ransomware Domains Using DNS Threat Intel

The most effective way to deal with Ransomware is to prevent users from accessing ransomware domains in the first place. Phishing, one of the most used delivery methods for ransomware, lure users to domains owned by threat actors.



Proactive identification of such domains, even before they are weaponized, is something that DNS threat intel excels at, because it can identify when domains are registered for future malicious purposes and block them, on an average of 63 days ahead of attacks.

Detecting C2 and Data Exfiltration Using DNS Threat Intel and DNS Behaviour Monitoring

By monitoring DNS traffic and using DNS threat intelligence, organizations can block the C2 communications, preventing the encryption key download and the eventual encryption of data. Blocking C2 at DNS ensures that the session is not even established with the attacker-controlled server, providing mitigation at the earliest possible opportunity.

Detecting data exfiltration over DNS involves monitoring an organization's DNS traffic in real time for unusual patterns, such as high-frequency queries to uncommon domains or queries with high entropy in their names. This behaviour-based analysis can identify data exfiltration to domains even if those domains are not yet categorized as malicious in threat feeds. It is important that all DNS record types are examined (e.g.: A, AAAA, CNAME, MX, NS, SOA, TXT, etc.) because malware could use any or multiple of these record types to avoid detection by standard security tools.

Proactive protection against ransomware is extremely important because once ransomware lands, organizations have only about an hour to detect, investigate and remediate to avoid a broader scale incident. Hence it is extremely critical to identify and stop C2 before the ransomware gets activated and propagates.

"DATA EXFILTRATION OVER DNS IS A SOPHISTICATED TECHNIQUE THAT ALLOWS ATTACKERS TO COVERTLY TRANSFER SENSITIVE DATA OUT OF AN ORGANIZATION BY LEVERAGING THE DNS PROTOCOL"

TECHBRIDGE MEA TO DISTRIBUTE CYWARENESS CYBER TRAINING PLATFORM IN THE MIDDLE EAST

Cywareness, a provider of AI-driven cyber awareness training solutions, has partnered with TechBridge MEA to distribute its platform across the Middle East and Africa, helping organizations combat the growing wave of cyberattacks in the region.

The Middle East continues to experience a surge in cyber threats targeting critical infrastructure, government institutions, and private enterprises. Alarmingly, research highlights that human error accounts for over 80% of cybersecurity breaches worldwide—a vulnerability that no amount of cutting-edge technology can completely shield.

Cywareness offers a solution by turning the weakest link into the strongest defense. Its comprehensive training platform equips employees with the knowledge to identify phishing attempts, social engineering tactics, and other cyber threats.

Organizations using Cywareness have reported:

- Fewer human errors thanks to practical, up to date, engaging training.
- Enhanced security culture across all levels of the organization.
- Simplified compliance through robust tracking and reporting.
- Improved training ROI through measurable, cost-effective solutions.

"Our platform transforms the human factor from a vulnerability into a strength," said Ari Lev, Sales Manager at Cywareness. "With multi-language customizable content and easy accessibility, we ensure every employee, no matter their role or background, is equipped to contribute to a safer workplace."

Steve Lockie, General Manager of TechBridge MEA, emphasized the importance of this partnership: "As digital transformation accelerates across the region, emaployee cyber awareness is no longer optional—it's critical. For our channel partners, Cywareness represents a unique opportunity to deliver scalable, high-demand solutions that strengthen client relationships and drive recurring revenue."

What Makes Cywareness Stand Out:

- AI-Powered Phishing Simulations: Realistic threat simulations via email, WhatsApp, and SMS.
- Updated Content Every 10-14 Days: Training stays relevant with updates tailored to emerging threats.
- Multi-Language Support: Eight dubbed languages and subtitles in any language for accessibility.
- ISO 27001 Certification: Meets the highest standards for information security.
- Compliance Tracking: Simplifies regulatory reporting for businesses.

As CVAD, TechBridge MEA sees tremendous value for its Channel Partner Community.

- Expand service offerings with an in-demand solution.
- Generate recurring revenue through subscriptions and ongoing training.
- Strengthen client retention with value-added services.
- Access comprehensive partner support and training resources.

As enterprises and governments in the Middle East increase their focus on cybersecurity and stricter data protection laws, the Cywareness-TechBridge MEA partnership arrives at a pivotal moment. Together, they aim to empower organizations to build robust security cultures while meeting the region's growing compliance requirements.

Cywareness is a leading cyber awareness training organization that uses AI-powered platform to help organizations reduce human error in cybersecurity through engaging, tailored, and effective training programs.

ring
an amazon company

etisalat and

Smart Monitoring Solutions

Free Lifetime Video Recording
3 Year Warranty
Free Installation
Free after-sales service

Keep an eye on your home even when you are away

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

Starts at AED 20*

For more information, lookup Smart Monitoring at www.etisalat.ae/smartmonitoring

*Terms and conditions apply

HIKVISION

EMBRACE AIoT FOR SAFER, SMARTER AND GREENER MOBILITY

Spot danger, stop risk

Detect and respond to incidents swiftly with advanced AI technology.

Streamlined Road Operation