ISSUE 89 | NOVEMBER 2024

WWW.TAHAWULTECH.COM

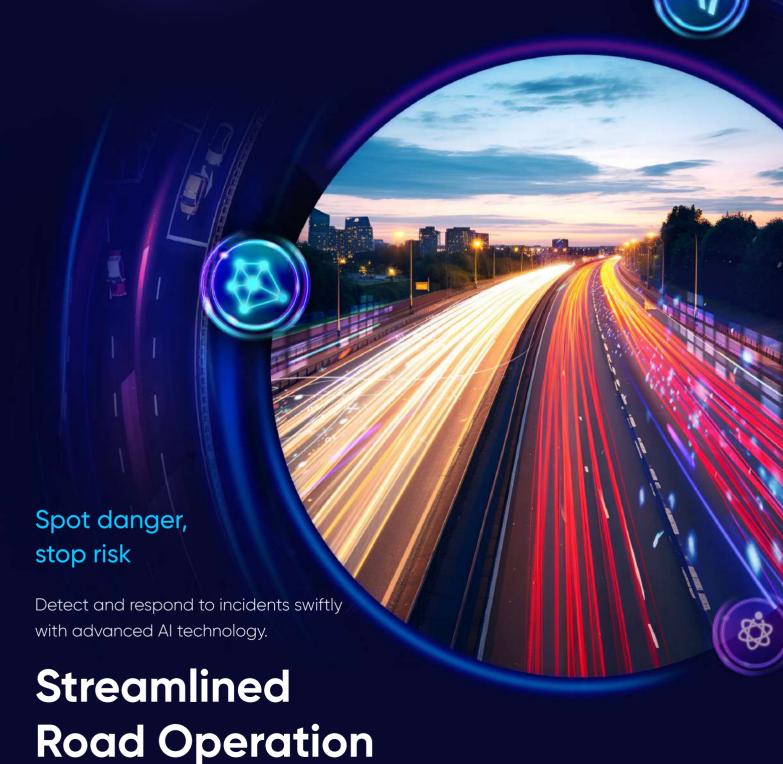
ADVISOR ADVISOR MIDDLE EAST

CYBERGUARD PIONEER NEXT-GEN DEFENSES

DISCOVER HOW THE MIDDLE EAST IS SETTING NEW STANDARDS IN CYBERSECURITY, OUTPACING GLOBAL TRENDS AND SAFEGUARDING DIGITAL FRONTIERS.

HIKVISION®





CONTENTS

Security

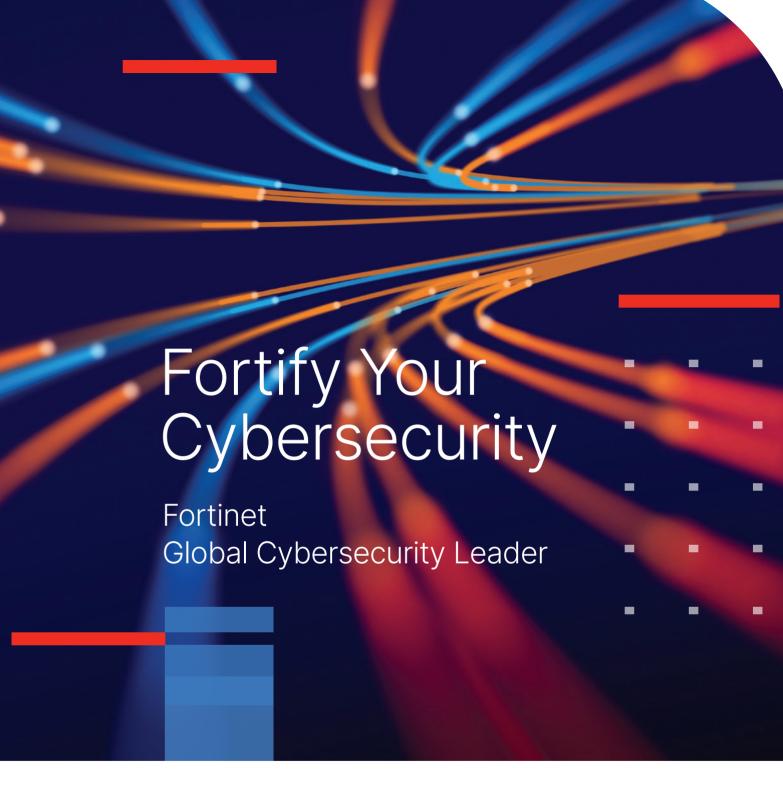








- News from the cybersecurity world in the region and beyond.
- Vectra Al:Tackling identity breaches and adopting cloud security innovation
- 20 OPSWAT Announced GITEX Global 2024 Pation Under Theme of 'Future Forward Critical Infrastructure Protection'
- 38 Middle Eastern firms surpass European counterparts in cybersecurity, says report by Securityscorecard.



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





EDITOR'S NOTE



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

Sandhya DMello Editor

EVENTS





CHARTING NEW FRONTIERS IN CYBERSECURITY

SECURE FUTURE

elcome to the November issue of Security ME magazine, where we traverse the evolving landscape of cybersecurity, illuminated by recent accomplishments and ongoing challenges. This edition draws attention to the substantial strides Middle Eastern companies are making in fortifying their cyber defenses, showcasing a remarkable resilience that sets a global benchmark.

Our story, informed by a recent for digit
SecurityScorecard analysis, reveals a telling
comparison: only 2% of Middle Eastern
companies reported direct cybersecurity
breaches in the past year,
markedly less than the 18%

SHAPING BRIGHT.

markedly less than the 18% in Europe. This striking disparity not only highlights

the effective security measures in place but also emphasizes the region's proactive approach to digital safeguarding. However, vulnerabilities within third-party ecosystems persist as a significant concern, with 84% of companies acknowledging breaches, suggesting a critical area for enhanced focus.

Telecommunications emerge as the most vulnerable sector, with a concerning 86% of companies rated C or lower in their cybersecurity practices. Contrastingly, the utilities sector stands out as a paragon of security, with no entities scoring below a C

and zero direct breaches, setting a standard for others to emulate.

Adding depth to our coverage, we spotlight initiatives by leading entities like Proofpoint, which has documented considerable progress among Middle Eastern retailers in fortifying their defenses against email fraud. Our report includes a detailed DMARC analysis that shows a robust adoption of preventative measures, setting a precedent for digital commerce security.

Looking ahead, the anticipation builds for Black Hat MEA 2024 in Riyadh. This event promises to be a pivotal gathering of

over 300 cybersecurity experts, including trainers and ethical hackers, poised to share their knowledge and shape the future

of cybersecurity practices.

This issue also features exclusive insights from industry leaders like Ranjith Kaippada of Cloud Box Technologies, who discusses the importance of aligning cybersecurity frameworks with business objectives.

Each article and interview in this issue is designed not just to inform but to inspire a proactive dialogue on enhancing cybersecurity measures.

Thank you for joining us on this journey through the dynamic world of cybersecurity. Together, we continue to build a safer digital environment for all.

FOUNDER, CPI Dominic De Sousa (1959-2015)

Published by



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

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com Editor Sandhya DMello sandhya.dmello@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, UAF

Tel: +971 4 5682993

© Copyright 2024 CPI All rights reserved

SECURE DOMAINS LAUNCH OPERATIONS IN THE MIDDLE EAST

Secure Domains, the first cloud native cybersecurity platform in the GCC specializing in DNS security, today announced the launch of its operations in the Middle East and Africa. As a cloud native cybersecurity vendor, Secure Domains helps organizations protect their users, data, and applications against advanced threats in a borderless infrastructure. The company is also the first vendor in the GCC to deliver unparalleled cloud-based DNS security services through its flagship SaaS product, DNS Armor.

"DNS security is crucial in today's cybersecurity landscape due to its critical role in preventing cyberattacks. The launch of our operations marks a significant step in Secure Domains' commitment in reshaping the cybersecurity and tech industry across the GCC and Africa region leveraging AI and ML. We are a customer centric organization fully focused on delivering key values related to reducing cyber risk, increasing productivity and optimizing cost while maintaining compliance." said Wissam Saadeddine. Co-Founder of Secure Domains. With 90% of cyber threats leveraging DNS in the cyber kill chain, DNS Armor positions itself as a critical first line of defense for businesses. Combining advanced threat intelligence with Al-driven DNS security, DNS Armor proactively blocks malicious domains,



detects DNS tunneling, and prevents data exfiltration. DNS Armor empowers organizations to take a proactive approach to cybersecurity, leveraging artificial intelligence (AI) and machine learning (ML) to stay ahead of evolving threats and safeguard sensitive data "As organizations in the region undergo digital transformation and adopt emerging technologies like SD-WAN and cloud computing, their security exposure expands. This leaves connected devices and networks more vulnerable to a range of cyber threats. We are excited to bring our expertise and advanced solutions to help organizations safeguard their operations against evolving cyber threats. We also look forward to supporting the



UAE's journey towards a more secure digital future," Mohammed Al Tenbakji, Co-founder of Secure Domains added. DNS Armor is built to support Managed Service Providers with flexible, scalable multi-tenancy, allowing IT teams to protect the organization anytime, anywhere while adhering to business policies. DNS Armor is fully operational across 25 data centers strategically located in the US, Europe, Asia, Middle East and Africa, enabling global reach and robust service delivery. With its headquarters in the UAE, Secure Domains is well-positioned to provide comprehensive coverage and support across the Middle East and North Africa region and beyond.

GCG ENTERPRISE SOLUTIONS BOLSTERS IT PORTFOLIO BY PARTNERING WITH FORENZY NETWORKS

GCG Enterprise Solutions, which serves from within Ghobash Group – a leading and diversified UAE-based business conglomerate has announced its strategic partnership with Forenzy Networks, a premier cyber security and digital forensics company. This collaboration aims to enhance GCG

Enterprise Solutions' IT Services department's capabilities in providing cutting-edge cybersecurity solutions.

The globally certified Forenzy Networks team includes CEH, CREST, and OSCP certified professionals, who ensure top-notch cyber security proficiency and excel in the identification and mitigation of modern cyber threats using advanced tools and techniques. They help organizations to safeguard their digital assets by utilizing years of Vulnerability Assessment and Pentesting experience, via a host of managed offerings including vCISO Services, Website Vulnerability Assessment & Penetration testing, Network

Vulnerability Assessment & Penetration testing, Red-Teaming, Cloud Auditing & Security Compliance measurement, along with Android & iOS Security Auditing.

As a leading Cyber Security as a Service (CaaS) provider with Digital Forensics expertise, covering the 360-degree landscape of security plus forensics, the company also specializes in securing Government infrastructure and data centers, further strengthening the resilience of critical systems and data.

Speaking on the development, Forenzy Networks' CEO - Bhaumik Merchant stated that: "We aim to deliver a one-touch platform that helps to discover, identify, assess, remediate and effectively monitor an organization's infrastructure, in order to keep it secure. Together with GCG Enterprise Solutions, we aim to deliver our unique brand which blends cyber security and digital forensics to a wider base of clients across the UAE".

"We welcome the addition of Forenzy Networks to our IT Services portfolio. Our enhanced focus on cyber security services is aimed at meeting the growing demand of regional businesses and we are very excited about the capabilities which Forenzy Networks delivers. We look forward to a mutually beneficial relationship which will set new benchmarks for cyber security excellence", added Hassan Allahham - Service Head, GCG Enterprise Solutions.

The Forenzy networks team is credited with facilitating international compliance with over 2,000 audits across 30+ locations worldwide, as well as for auditing government infrastructure and contributing to some very prestigious cybersecurity standards, including G20 Summit initiatives

SPLUNK CLOUD NOW AVAILABLE ON AWS UAE – A GAME-CHANGER FOR REGIONAL DIGITAL TRANSFORMATION

Splunk, a Cisco Company and the cybersecurity and observability leader, recently announced the official launch of Splunk's Cloud offerings on Amazon Web Services (AWS) Middle East in the UAE region, with Splunk Cloud Platform (SCP), Enterprise Security (ES) and Splunk IT Service Intelligence (ITSI) now available.

This highly anticipated launch responds to the growing demand from organisations in the Middle East for locally-provisioned Splunk services.

With the launch of Splunk Cloud on AWS UAE, businesses across the region can now access the full power of the Splunk Enterprise Platform as a scalable SaaS solution on AWS' highly secure cloud infrastructure.

Splunk Cloud on AWS UAE offers security, IT and DevOps teams real-time visibility into their operations, enabling them to proactively identify and resolve potential issues before they escalate. This helps minimise downtime and ensure business continuity, all while reducing latency and providing faster access to critical data for more informed decision-making.

splunk>

a CISCO company organisations. Not only does it

Beyond the core Splunk Cloud Platform, businesses will also benefit from advanced solutions such as Enterprise Security (ES) and IT Service Intelligence (ITSI). These tools enhance threat detection, security response and the performance monitoring of key business services, empowering organisations to optimise their IT infrastructure and improve overall operational efficiency.

This also enables Middle Eastern organisations to meet customer expectations for local presence with a trusted, transparent, responsible, and secure by design solution. Splunk Cloud enables businesses and governments to confidently pursue digital transformation initiatives and data-driven outcomes, and embrace the region's spirit of innovation, while maintaining data locality.

Ahmed El Saadi, Vice President for Middle East & Africa at Splunk, emphasised the impact of this launch: "The introduction of Splunk Cloud in the UAE is a game-changer for regional organisations. Not only does it enable data locality, but it also

empowers businesses with real-time, Al-driven insights that can significantly enhance their IT and security operations. By reducing latency, enhancing decision-making and providing unmatched operational agility, Splunk Cloud will be a cornerstone for organisations in the Middle East looking to lead in their industries and drive digital innovation in an increasingly competitive landscape".

The availability of Splunk Cloud in the UAE marks a significant milestone in Splunk's mission to drive responsible digital innovation across key industries such as aviation, logistics, government, and FSI. Through automation, AI-powered insights and real-time data analytics, Splunk empowers businesses and government entities across the Middle East to achieve operational excellence and long-term digital resilience.

KASPERSKY REPORTS NEARLY 25% SURGE IN RETAIL-FOCUSED CYBERTHREATS AHEAD OF BLACK FRIDAY

In 2024, cybercriminals launched over 38 million phishing attacks, impersonating major marketplaces, banks, and tech retailers. Stolen payment card data is actively traded on dark web forums, with prices ranging from \$70 to \$315 per set.

Kaspersky closely monitors the evolving landscape of shopping-related cyber threats. As shoppers prepare for major sales events like Black Friday in search of the best deals, the company's researchers observe cybercriminals and fraudsters gearing up to exploit this demand, attempting to steal personal data, funds, and spread malware through deceptive shopping lures.

Between January and November 2024, Kaspersky solutions blocked 38,473,274 phishing attacks related to online shopping, payment systems, and banking institutions. Of these, 44% involved using banking services as bait — representing an increase of almost a quarter compared to the 30,803,840 million phishing attempts recorded during the same period last year.

Scammers frequently impersonate major retailers like Amazon, Walmart, and Etsy, sending deceptive emails claiming to offer exclusive discounts. These emails link to fake websites designed to mimic legitimate ones, often with subtle errors like misspellings or slightly altered domain names. Victims attempting to shop on these sites typically lose money.

Another widespread scam exploits consumers' desire to win prizes. Fraudsters send messages promoting limited-time surveys with prize draws, offering valuable rewards like a free iPhone 16. To create urgency, they claim only a few "chosen" users can access the deal, pressuring recipients to act quickly. Scammers offer a "reward" for sharing some "basic info," such as an email address, and spending some money on a fake site.

Kaspersky experts have traced the pathways of fraudulent activity, revealing that stolen data is either exploited directly by scammers or sold on dark web marketplaces. The value of the data determines its price. For instance, comprehensive sets of stolen credit card details, known as "fullz," typically include the card number, expiration date, CVV code, cardholder's name, billing address, and phone number.

AXIS COMMUNICATIONS LAUNCH ARTPEC-9 SOC, FEATURING SUPERIOR PERFORMANCE, AV1 VIDEO ENCODING SUPPORT

Axis Communications, the global leader in security and network surveillance technologies, has announced the 9th generation of its purpose-built system-on-chip (SoC). ARTPEC-9 builds on and refines the capabilities and features of previous generations of the company's in-house designed SoC, including exceptionally low bitrate, AI-powered analytics, quality imaging, and enhanced cybersecurity.

In a first for network video, ARTPEC-9 now supports the proven AV1 video encoding standard from the Alliance for Open Media (AOM). Together with Axis Zipstream, AV1 reduces data storage costs without sacrificing forensic detail.

"ARTPEC-9, with its industry-first support for AV1, allows for attractive bitrates and extended client compatibility. It's really a win for the industry," said Johan Paulsson, Chief Technology Officer at Axis Communications. "The keywords are 'easy access' and 'open', which align perfectly



with how we work to fulfil our promise of innovating for a smarter, safer world. Plus, like all our SoCs, ARTPEC-9 is made expressly for high-quality network video. And, as always, we retain complete control of the SoC production process."

Axis will begin including the ARTPEC-9 SoC in select network video products starting in early 2025.

Superior performance, delivering highquality results ARTPEC-9 boosts the powerful signature technologies that have long facilitated market-leading Axis image processing under difficult light conditions, including Axis Lightfinder and Axis Forensic Wide Dynamic Range (WDR). These solutions form part of the foundation for Axis Scene Intelligence technology, which increases the performance of analytics applications.

The outcome is consistent analytics results and fast, accurate forensic search capabilities with minimal false alarms, even under challenging surveillance conditions. ARTPEC-9, along with Axis' decades of experience with image processing, means security teams will achieve reliable, high-quality results in any situation.

A new standard in video encoding

With ARTPEC-9, Axis has introduced AV1, the next-generation open video encoding standard for streaming media to the surveillance industry. Support for AV1 and enhanced image processing mean

ARTPEC-9 delivers high-quality video with uncompromised detail and clarity and best-in-class bitrate.

Together with Axis Zipstream, AV1 ensures hassle-free video both on-premises and in the cloud. AV1 is currently supported by AXIS Camera Station.

Providers of major video management solutions (VMS) like Genetec and Milestone will be adding support for AV1, with further developments already underway.

'See' more with analytics

ARTPEC-9 opens the door for more advanced Al analytics with increased performance that 'see' further away. In other words, analytics that detect smaller objects and trigger alarms and notifications earlier to deliver actionable insights for security, safety, and operational purposes.

Other improvements include higher accuracy and analytics that recognise and differentiate between more object classes

for more granular and nuanced object classification.

Strengthened cybersecurity

Cybersecurity is at the core of ARTPEC-9's design. Features like secure boot and signed OS ensure that each device remains protected from cyberthreats. Additionally, since ARTPEC-9 is developed in-house, Axis retains full control over the production process, further strengthening device security.

FROM QR CODE TO COMPROMISE: THE GROWING THREAT OF "QUISHING"

Sophos, a global leader of innovative security solutions for defeating cyberattacks, today released the results of Sophos X-Ops research on a new type of threat: quishing. This new attack vector involves the use of fraudulent QR codes, emailed by threat actors, to bypass the phishing security measures put in place by companies.

This fraudulent QR code, embedded in a PDF document attached to an email. takes the form of a message about payroll, employee benefits, or other forms of official paperwork a business might send to an employee. Because QR codes are not readable by computers, the employee must scan the QR code using their mobile phone. The QR code links to a phishing page, which the employee may not recognize as malicious since phones usually are less protected than a computer. The goal of the attackers is to capture employees' passwords and their multi-factor authentication (MFA) tokens in order to access a company's system by bypassing the security measures in place.

"We spent a considerable amount of time sifting through all the spam samples we had to find examples of quishing," said Andrew Brandt, principal researcher at Sophos X-Ops. "Our research has revealed that attacks that exploit this specific threat vector are intensifying, both in terms of volume and sophistication, especially when it comes to the appearance of the PDF document.

In addition to social engineering tactics, the quality of emails, attachments and QR code graphics, these attacks seem to be growing in terms of organization as well. Indeed, some

malicious actors now offer as-a-service tools to run phishing campaigns using fraudulent QR codes. In addition to features such as CAPTCHA bypasses or the generation of IP address proxies to bypass automated threat detection, these criminal organizations provide a sophisticated phishing platform that can capture the credentials or MFA tokens of targeted individuals.

To encourage organizations to better protect systems against this type of attack, Sophos X-Ops shares a list of recommendations:

Be vigilant about internal emails about HR topics, salaries or company benefits: Sophos X-Ops' research has found that social engineering tricks exploit these themes to trick employees into scanning fraudulent QR codes from their mobile devices.

Install Sophos Intercept X for Mobile: Available on Android, iOS and Chrome OS, this solution includes a secure QR code scanner that helps identify known phishing websites and alert if the URL is considered malicious.

Monitor risky sign-ins: Using identity management tools, organizations can detect unusual sign-in activity.

Enable Conditional Access: This feature helps enforce access controls based on the user's location, device status and risk.

Enable effective access monitoring thanks to sophisticated logs: this type of advanced monitoring allows you to better visualize all access to the system and detect this type of threat in time.

Implement advanced email filtering: Sophos' QR code phishing protection solution



detects fraudulent QR codes included directly in emails and plans to expand its solution to QR codes in attachments as early as the first quarter of 2025.

Leverage on-demand email retrieval: Sophos Central Email customers who use Microsoft 365 have this feature to eliminate spam or phishing emails from corporate emails.

Encourage employees to be vigilant and report incidents: Prompt reporting of anomalies to the incident response team is essential to protect company systems from phishing.

Revoke suspicious user sessions: It is imperative to have a plan in place to revoke user access that shows signs of compromise.

Despite the continuous development of new attack vectors, organizations can protect themselves from compromised systems by equipping themselves with the right tools, fostering a culture and work environment, and surrounding themselves with security vendors that, like Sophos.

BLACK HAT MEA 2024: Program Runni SPEARHEADING CYBERSECURI INNOVATION IN RIYADH

lack Hat Middle East & Africa (MEA) will raise a bar higher this year as cybersecurity experts from around the world land in Saudi Arabia to attend the three-day power-packed display of latest solutions in cybersecurity.

Black Hat, a premier global player in cybersecurity events and information security training, established its Middle East & Africa edition in 2022. This edition attracted over 30,000 information security professionals from more than 100 countries to Riyadh, aligning with the region's ambitious ICT security growth under Vision 2030.

Black Hat MEA offers comprehensive

ethical hacking courses and offensive security training year-round. The event spans three days and includes an Executive Summit, Briefings, an Arsenal, a Business Hall, and an interactive Activity Zone with prize funds totaling up to SAR 1,000,000. Black Hat MEA serves as a vital capacity-building platform in the region, drawing top-tier information security experts to train attendees and fortify Vision 2030 against emerging cyber threats.

This year discover the forefront of cybersecurity expertise at Black Hat MEA 2024 in Riyadh, KSA. Join 300+ global cybersecurity influencers and experts, 30 Black Hat trainers, and hundreds of ethical hackers.

Black Hat Middle East & Africa (MEA). one of the world's leading cybersecurity conference and exhibitions, has already locked in some of the biggest names in information security to speak at this November's Executive Summit.

From Silicon Valley to São Paulo, top innovators, investors, and ethical hackers have been confirmed for this year's event, which will run from November 26-28 at the Rivadh Exhibition & Convention Centre in Malham. Discussing the global evolution of cybersecurity and its latest developments – such as quantum computing & cryptography, supply chain security, remote workforce security and threat detection responses - the annual Executive Summit will see more



than 100 Chief Information Security Officers (CISOs) and other executives in attendance.

Many of these senior IT leaders are in charge of security for some of the largest organisations in the world and will use Black Hat MEA 2024 to share their insights and experience.

The initial line-up includes: Gary
Hayslip, Chief Information Security
Officer, SoftBank Investment Advisors;
Lori Wade, IC Chief Data Officer, Office
of The Director of Intelligence; Sounil
Yu, Founder & Chief Technology Officer,
Knostic; Kevin Jones, Global Chief
Information Security Officer, Bayer
Group; Jennifer Ewbank, former Deputy
Director, Digital Innovation, Central

Intelligence Agency; Jason Lau, Chief Information Security Officer, Crypto.Com; Rich Baich, Chief Information Security Officer, AT&T; Ashish Shrestha, Chief Information Security Officer, Jaguar Land Rover; Lakshmi Hanspal, Strategic Advisor & Investor, Silicon Valley CISO Investments; and Craig McEwen, Deputy Chief Information Security Officer & Global Head of Cyber Technology & Operations, Unilever.

"The cybersecurity goalposts have moved and now, more than ever, keep on moving as our industry faces some of its biggest challenges due to the evolving nature of threats", said Annabelle Mander, Senior Vice President of Tahaluf – organisers of Black Hat MEA in partnership with the Saudi Federation for Cybersecurity, Programming and Drones (SAFCSP). "From AI and machine learning to interconnected technologies and humans, who continue to be one of the biggest threats to organisations, the pace of change is extraordinary".

"At Black Hat MEA 2024, our experts will put all this – and their related risks – into perspective and signpost potential solutions", added Annabelle. "Tahaluf is building on last year's event by moving to a larger venue to accommodate the increased demand from exhibitors and visitors, keen to hear from and connect with some of the leading names from the cybersecurity sector industry across three days. The KSA is becoming a

hub for cybersecurity excellence and therefore we look forward to welcoming some of the world's biggest names in this sector to Black Hat MEA in November".

Black Hat MEA is also lining up an exhibition of regional and global cybersecurity leaders and innovators, including some of the sector's biggest names. The line-up already includes Kaspersky – which successfully blocked 30 million cyber threats in the UAE last year – Fortinet, Opentext, Builder AI, Help AG, Infoblox, Netwitness, Palo Alto Networks, Recorded Future, and Trend Micro.

Black Hat MEA 2024 will be packed with all the interactive features that have seen the event now rank amongst the world's biggest cybersecurity exhibitions. These include industry briefings and training sessions, the Cyberseed start-up competition, an investor programme, and the Black Hat MEA Arsenal, in which developers showcase the latest open-source tools and products. In partnership with ToolsWatch, the Black Hat MEA Arsenal will also see presenters interacting with attendees for firsthand experiences. In addition, information security experts will share new industry

tricks and trends, and hackers will expose the latest breach techniques. The event will also encompass the Black Hat Campus, which is an area for entry level professionals to attend talks and meet industry experts to understand how they can grow their career in cybersecurity.

The exhibition's Activity Zone will also host a jeopardy-style Capture The Flag tournament, with over 1000 participants competing in a series of challenges across various competency levels. In addition, the Cyberseed Start-up Competition will host pitches from startup teams, who will compete for a share of the Cyberseed Prize Fund. The competition will have multiple mentoring sessions where finalists will get to present their ideas to an esteemed set of judges.

Explaining Trend Micro's participation at the Black Hat MEA 2024, Dr. Moataz Bin Ali, Regional Vice President and Managing Director, Mediterranean, Middle East, Eurasia & Africa at Trend Micro, added:

"At Trend Micro, we are honoured to participate in an event that embodies technological advancement and excellence. Events like Black Hat MEA are stepping stones to realising Saudi

Vision 2030, fostering technological growth and cybersecurity resilience. We look forward to unveiling our latest innovations and engaging in dialogues that will shape the future of cybersecurity".

Cisco is participating as a Strategic Sponsor at Black Hat MEA 2024 under the theme "Innovating a New Era of Security," showcasing its latest innovations in cybersecurity. This year, Cisco is highlighting how it powers and protects the engine of the AI revolution – AI-ready data centres and clouds – to make every application and device secure no matter how they are distributed or connected.

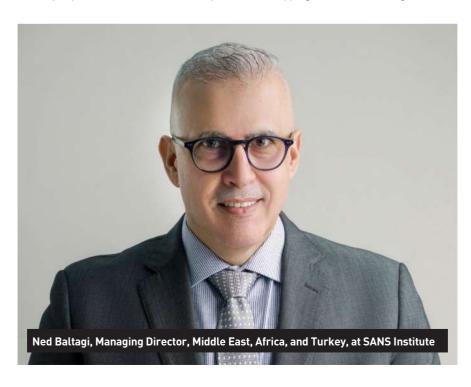
Salman Faqeeh, Managing Director, Cisco Saudi Arabia, commented: "The mounting trends in identity-based attacks and ransomware highlight the evolving nature of cyber threats. At Cisco, we are committed to supporting our customers in strengthening their digital resilience with advanced security solutions." He added, "Black Hat MEA continues to be a significant platform for us to share latest threat insights and showcase our innovations that prevent identity-based attacks; detect and stop breaches; and close the exploit gap."

Additionally, Splunk, a Cisco company, will showcase its innovations at the same booth, demonstrating solutions that support the future of Security Operations Centres (SOC) as well as specialized solutions for Operational Technology (OT) environments.

As part of Cisco's program of events at Black Hat MEA, Lothar Renner, Managing Director, Cisco Security, EMEA, will deliver a keynote address on "Redefining Security in the Age of AI," emphasizing Cisco's commitment to innovation and security in an increasingly complex threat environment.

Cisco will be present at booth H1-T20 at the Riyadh Exhibition & Conference Centre in Malham from 26-28 November 2024.

Tom Lowndes, Regional Director, Middle East, CyberArk, said: "Saudi Arabia is a very important market for CyberArk



in the Middle East. We have been experiencing growth of about 25% year-on-year in Saudi since we launched our services in the region over six years ago."

Saudi Arabia is accelerating rapidly as part of that growth and now makes up about 40% of CyberArk's Middle East business. We have more than 50 customers in Saudi Arabia including some of the biggest names in finance, government, and manufacturing. Our customer base continues to grow, with an average of five new customers joining every quarter.

Cora Al, Secrets Management

CyberArk will be showcasing major solutions at Black Hat MEA, with a particular emphasis on Cora AI, Secrets Management, and machine identity solutions from Venafi, which the company acquired earlier in the year. The company is exhibiting with Gulf IT in Hall 1, stand Q10, and Help AG in Hall 1 – J30 & Hall A3-H1-Q10.

"Our solutions are vital to help companies cope with a fast-changing threat landscape, with the rise in the number of human and machine identities having transformed the threat landscape



in Saudi Arabia and globally in 2024. We are making significant investments in Saudi Arabia, and we want to enable our full platform and establish a local presence in the country within the next 18 months. This will enable end-to-end holistic identity services and allow us to focus on helping customers reduce the number of tools they use and lower

their cyber debt. This is important as the average Middle East customer uses 10 tools to manage identity security, which causes unnecessary complexity and weakness. We want to double the size of our business in Saudi Arabia in the next 12-24 months," added Lowndes.

15-minute NetWars tournaments

At Black Hat MEA 2024, SANS Institute is showcasing its expertise in bridging the global skills gap, highlighting its portfolio of practical cybersecurity training solutions and programs. Ned Baltagi, Managing Director, Middle East, Africa, and Turkey, SANS Institute, said: "We will be holding a series of 15-minute NetWars tournaments at the booth, and this interactive competition will give visitors first-hand experience with how our hands-on training programs prepare cybersecurity professionals to tackle real-world challenges immediately. Our presence reflects our commitment to supporting Vision 2030 - Saudi Arabia's roadmap to economic diversification and digital transformation – and upskilling professionals in the Middle East and beyond. SANS is helping to develop a highly skilled cybersecurity workforce, essential for protecting the Kingdom's



infrastructure and digital economy."

Autonomous SOC technology

At Black Hat MEA 2024. SentinelOne will present its latest advancements in autonomous SOC technology. designed to streamline and enhance security operations. Key innovations include Singularity Hyperautomation, Singularity AI SIEM, and cutting-edge capabilities in Purple AI, its generative Al-powered security analyst. SentinelOne will showcase its Singularity Platform, featuring Al-powered threat detection, response, and recovery capabilities. Visitors can experience live demos of autonomous EDR/XDR. ITDR solutions. and seamless integrations with leading security ecosystems.

Meriam ElOuazzani, Senior Regional Director META, SentinelOne, said: "As Saudi Arabia advances towards Vision 2030, SentinelOne is set to help organizations achieve future-proof security aligned with the Kingdom's digital transformation and cyber resilience goals. Our innovations are purpose-built to deliver scalable, automated protection against sophisticated threats, focusing on



securing critical infrastructure, empowering SOC teams, and simplifying cyber defenses. Black Hat MEA offers us a key opportunity to connect with cybersecurity leaders, CISOs, and experts, share our expertise, and strengthen our commitment to local organizations and beyond."

Al-powered Cloud Security solution

Tenable will showcase its Al-powered Cloud Security solution, supporting Saudi Arabia's Vision 2030. This CNAPP solution helps reduce risk by rapidly exposing and closing priority security gaps caused by misconfigurations, risky entitlements and vulnerabilities—across multi-cloud platforms such as GCP, AWS, Azure and OCI. Tenable will also share insights from its 2024 Cloud Risk Report, highlighting the "toxic cloud trilogy"—a risky combination of critical vulnerabilities, excessive permissions, and public exposure—impacting 38% of organizations globally.

"Tenable helps expose and close security gaps across converged IoT, OT, and IT environments," said Maher Jadallah, VP of MENA at Tenable. "Our team will assist visitors in understanding and mitigating these risks."

Sophos Firewall

Sophos will highlight latest advancements in cybersecurity, including Sophos Firewall, which offers network security with advanced threat protection, web filtering and secure VPN access, ensuring that businesses can protect



their networks from even the most sophisticated attacks.

"At Sophos, we are committed to advancing Saudi Arabia's cybersecurity landscape with our innovative solutions driven by AI. We will also focus on Sophos Managed Detection and response (MDR), a comprehensive threat detection service that combines machine learning and expert human analysis. By integrating Sophos Firewall with Managed Detection and Response (MDR), we aim to deliver comprehensive end-to-end security solutions that align seamlessly with the Kingdom's strategic vision for a resilient and secure digital infrastructure," said Harish Chib, VP Emerging Markets, Middle East & Africa, Sophos.

Nozomi Arc

Nozomi Networks will highlight its latest innovations, including Nozomi Arc, and Threat Intelligence Feed 3.0, all tailored to secure OT/IoT environments across energy, oil and gas, and utilities. The company will also emphasize its key role in helping organizations in the Middle East meet regional compliance standards, including the NCA requirements and OT Cybersecurity Controls (OTCC) framework.

"Black Hat MEA is a premier gathering of cybersecurity professionals and innovators, and our goal is to connect with regional leaders and showcase how our solutions can protect critical networks, from energy to transportation, against the unique cyber threats facing OT and IoT environments here. With our expanded portfolio of regionally adapted solutions, we are here to support Middle Eastern organizations as they navigate the complexities of securing critical infrastructure at a time where AI is reshaping cybersecurity. We are also working towards contributing to the



growth of the Kingdom's cybersecurity sector in alignment with Vision 2030, addressing the growing convergence of IT and OT security," said Khalid Aljamed, VP KSA, Nozomi Networks.

Black Hat MEA is working together with the Saudi Federation for Cybersecurity, Programming and Drones (SAFCSP) to deliver one of the world's largest and most iconic cybersecurity events, helping build capabilities and nurture talent in the cybersecurity field.

Aside from the fact that the event brings together top cybersecurity experts and thought leaders from across the public and private sectors, both regionally and globally, Black Hat has also made its name in the annual event calendar thanks to its incorporation of unique, interactive and exciting features such as Hackathons and Capture the Flag competitions.

As one of the most well-attended technology conferences in the Middle East, Black Hat is a microcosm of Saudi Arabia's broader efforts to be a global tech and cybersecurity hub, in line with government initiatives like the National Cybersecurity Strategy, which ultimately feed into Saudi Vision 2030.

Safwan Akram, VP Service Operations - KSA, Help AG, said: "We are glad to join this vital and important industry platform once again, following our event debut last year. At the 2024 edition of Black Hat MEA, Help AG will spotlight our advanced cybersecurity services and solutions combining cutting-edge tech with local expertise. Our presence reflects our commitment to securing the Kingdom's digital transformation journey under Vision 2030."

Help AG's stand — in Hall 1 – Stand J30 — will feature an innovation zone where visitors can experience live demos and insights into enabling safe, responsible AI integration and introducing quantum-resistant encryption – key elements of Help AG's futuristic Cybersphere Nexus. Visitors can also explore our end-to-end portfolio, including services such as Managed Cyber Defense, Digital Risk Protection, Digital Forensics and Incident Response, Cloud Security, Data and Identity Protection, Offensive Security, and Governance, Risk, and Compliance.

GLOBAL EXPERTS GATHER TO NAVIGATE THE FUTURE OF CYBERSECURITY AT THE FOREFRONT OF TECHNOLOGICAL ADVANCEMENT"



AHMAD FIDA WELDALI.

REGIONAL SALES DIRECTOR AT LINKSHADOW, DISCUSSES HOW CONTINUOUS INNOVATION, TRAINING AND EMPOWERMENT ARE EQUIPPING THEIR CHANNEL PARTNERS TO FACE THE FUTURE WITH CONFIDENCE.

et's dive into the
evolving landscape of
channel partnerships
in cybersecurity with
LinkShadow. How does

LinkShadow approach its channel partners?

Organisations are increasingly relying on partner programs to expand their reach, deliver innovative solutions, and drive business growth. At LinkShadow, we have developed a comprehensive and robust partner program with LinkShadow Cyber Mesh Platform Solution to empower our partners and maximise mutual growth and success.

LinkShadow recognises the importance of equipping its partners with the necessary knowledge and tools to effectively sell and support LinkShadow AI Powered cybersecurity solutions to customers. Our partner program offers comprehensive training and certifications, enabling our channel partners to enhance their technical expertise and stay up-to-date with the

latest industry trends.

This includes ongoing product training, sales enablement, and access to a dedicated partner portal with a wealth of resources, including sales collateral, technical documentation, and marketing materials.

How exactly does LinkShadow support its channel partners in enhancing their capabilities?

Empowering partners to drive success is key. We have a comprehensive



onboarding and enablement program designed to equip them with the knowledge and tools needed to succeed. This includes free technical certification, access to our product portal, and real-time reporting capabilities that enable partners to provide value-added services using LinkShadow AI Powered Cyber Mesh Platform to their customers.

LinkShadow understands the importance of providing reliable technical support to its partners and

their customers. The partner program offers access to a dedicated technical support team, ensuring prompt resolution of any product-related queries or issues. This collaboration extends to joint solution development and coselling initiatives, enabling partners to leverage LinkShadow's expertise and resources to deliver comprehensive LinkShadow cybersecurity solutions such as NDR, UEBA, OpenXDR, DSPM using Linkshadow Cyber Mesh Platform to their customers.

What are some of the main challenges businesses in the region face when it comes to cybersecurity?

The challenges are multifaceted. A significant issue is the shortage of skilled cybersecurity professionals, which affects organisations globally. Additionally, many businesses struggle with vendor lock-in, where they are tied to specific solutions that hinder their flexibility. We address this by ensuring that through the Cyber Mesh platform LinkShadow can integrate with a variety of existing security tools,



thus providing a more adaptable and holistic approach to cybersecurity and enabling customers to have the capability of solutions like NDR, UEBA, OpenXDR, DSPM Powered by Al under Linkshadow Cyber Mesh Platform.

Can you elaborate on the integration of AI within your security platform?

Absolutely. The LinkShadow Cyber Mesh Platform uses AI to automate the correlation of data from various security tools. This not only streamlines the process of threat detection but also enhances compliance management. As regulations become increasingly stringent, having a centralised view of compliance-related data is crucial for organisations. We are not just focused on security; we are also addressing data governance and compliance, which are essential for businesses today.

Compliance is indeed a major concern. How does LinkShadow ensure that its partners can support clients in meeting these regulatory requirements?

We empower our partners by providing them with tools that facilitate compliance monitoring. LinkShadow Cyber Mesh Platform can generate reports that help organisations demonstrate compliance with local data protection laws. For example, it can pinpoint where the sensitive data resides and who has access, ensuring that customers can quickly respond to audits and compliance checks, LinkShadow's latest initiative in the Data Security space is primarily focused on helping organisation to manage Data Security / Privacy compliance using Linkshadow Data Security Posture Management (DSPM).

Education is also a significant factor, how does LinkShadow address the knowledge gap in the market?

We recognise the need for ongoing education and upskilling in cybersecurity. LinkShadow Cyber Mesh Platform is designed to be user-friendly, allowing organisations to develop their own AI models and adapt to new trends without requiring extensive technical expertise. We also encourage our partners to offer training and resources to their customers, fostering a more informed customer base. One of the key benefits is the On-Prem Custom AI Data Models, which customers can create, and fine-tune based on their own environments. This feature, referred to by LinkShadow as the AI-Powered Engine, requires minimal effort from the customer.

As organisations increasingly migrate to the cloud, how does LinkShadow ensure data security across various environments?

LinkShadow Cyber Mesh Platform provides visibility into both on-premises and cloud environments, helping organisations secure their data regardless of where it resides. By leveraging

LINKSHADOW REVEALS GAME-CHANGING DATA SECURITY SOLUTION

THE COMPANY'S LATEST SOLUTION PROVIDES ENHANCED CLOUD DATA VISIBILITY AND AI-POWERED PROTECTION.

At GITEX this year, LinkShadow made waves with the launch of its new Data Security Posture Management (DSPM) solution, a significant leap forward in safeguarding sensitive data across cloud environments. Known for its robust Network Detection and Response (NDR) capabilities, LinkShadow is now taking a proactive approach to address the evolving challenges of data security.

In an interview, Ahmad Fida Weldali, Regional Sales Director at LinkShadow, shared insights into the company's new offering and how it's reshaping the cybersecurity landscape. Weldali explained that while LinkShadow's NDR solution has been instrumental in detecting and responding to network-based threats, the DSPM solution addresses a different pain point—one that has become increasingly pressing as more organisations migrate to the cloud

"For a long time, people moving to the cloud couldn't find a solution that provided adequate visibility into their private and sensitive data. DSPM bridges that gap," Weldali said. The new solution gives organisations deep insights into where their sensitive data resides in cloud environments, ensuring better control and security over data that was previously invisible.

Weldali shared that the response at GITEX has been overwhelmingly

WITH DSPM, WE HELP CUSTOMERS LOCATE AND MONITOR THEIR SENSITIVE DATA, ENSURING COMPLIANCE WITH PRIVACY REGULATIONS.

positive. "So far, the response has been wonderful because this was the missing part. Whenever personal data moves to the cloud, organisations often lose track of where it goes. With DSPM, we help customers locate and monitor their sensitive data, ensuring compliance with privacy regulations."

When asked how LinkShadow is leveraging AI, Weldali said that the company's AI engine has been developed in-house, offering advanced capabilities such as detection, prioritisation, and correlation of network data. "Our AI engine processes information from the customer's network, consolidating it in a way that allows for faster and more accurate detection and response," he explained.

This Al functionality extends to the DSPM solution, where it plays a crucial role in data analysis. By correlating sensitive data across various sources, Al prioritises the data, identifies vulnerabilities, and maps out its movement within the cloud.

In the era of heightened data privacy concerns, the importance of keeping sensitive information secure cannot be overstated. LinkShadow's DSPM solution is designed with compliance in mind, ensuring that no sensitive data leaves the customer's environment.

Weldali emphasised: "We developed our AI engine to operate within the customer's virtual machine or hardware, so nothing ever leaves the customer's control. This guarantees that data remains secure and compliant with privacy laws. Without visibility into your data, you can't protect it."

As digital transformation accelerates and cloud adoption becomes the norm, cybersecurity challenges are becoming more complex. However, LinkShadow is staying ahead of the curve with DSPM, offering a solution that integrates seamlessly with its existing NDR capabilities to provide a comprehensive data security strategy.

"Everything in IT security ultimately comes down to securing the data," Weldali concluded. "With DSPM, we're not just securing the network—we're securing users and their data, delivering the visibility and protection they need today."

Al and a cyber mesh architecture, we enable clients to monitor their Network or Data security posture comprehensively and efficiently using NDR, UEBA, OpenXDR, DSPM services, which is essential in today's hybrid environments.

How do you foresee the future of cybersecurity partnerships evolving?

The future of cybersecurity partnerships will be centered around collaboration and flexibility. As threats continue to evolve, partners must be equipped to provide

innovative solutions that can adapt to changing regulatory landscapes and customers' needs. By fostering a strong partnership ecosystem and focusing on integration, we believe LinkShadow can help our partners thrive in this dynamic environment.

We are excited to continue our journey in the cybersecurity landscape and support our partners in delivering robust solutions to their clients. Our partner strategy is comprehensive and well-structured to empower the

channel community to drive business growth while delivering cutting-edge cybersecurity solutions to their customers. By providing extensive enablement, sales, and marketing support, technical collaboration, and attractive offers, LinkShadow ensures that its partners have the necessary resources and tools to succeed in today's competitive market. As a result, we are looking forward to creating a win-win scenario, and fostering stronger alliances that can drive mutual growth and joint success stories.



OPSWAT ANNOUNCED GITEX GLOBAL 2024 PARTICIPATION UNDER THEME OF 'FUTURE FORWARD CRITICAL INFRASTRUCTURE PROTECTION'

ON THE URGENCY TO ADDRESS IT-OT CONVERGENCE AND PROTECT WHAT MATTERS MOST

PSWAT announced its participation at GITEX Global 2024, under the theme "Future Forward CIP." Trusted by several of the region's governments and largest private sector entities, OPSWAT's participation at the 44th GITEX demonstrated its ongoing commitment to delivering cybersecurity solutions that span the OT-IT divide and gave security professionals the tools they needed to support mitigation of their threat vectors.

"Critical infrastructure calls for critical defence," warned Sertan Selcuk, Vice President of Sales for the Middle East, Turkey, Africa, Pakistan, and CIS at OPSWAT. "OPSWAT urged clients to trust no file or device. We believed it was only through this approach that we could eliminate malware, particularly zero-day exploits, and guard against attacks on our most vital IT and OT environments."

The central showcase of OPSWAT's GITEX booth was its Mobile CIP Lab where delegates got an in-depth understanding of the company's MetaDefender platform. Interactive demonstrations of region-specific use cases covered storage security, supplychain security, secure managed file transfer, peripheral and removable media

protection, access and endpoint security, email security, OT security, cross-domain security, and many others.

Visitors also toured OPSWAT's Nuclear Plant Model Reactor, which reinforced the company's credentials in securing the most sensitive industrial environments. GITEX visitors saw firsthand how OPSWAT's IT/OT platform deployment worked in real-world scenarios relevant to GCC critical infrastructure.

Selcuk said, "Faced with increasingly complex technology environments and relentlessly targeted by sophisticated attackers, yesterday's critical infrastructure security leaders had to think not only about detection, but about the perimeters of their organisation and how they guarded against peripheral media and endless file uploads; about how they implemented security for web applications and storage security; and about how they built a culture of awareness that allowed them to deliver the protections needed to maintain public trust".

While visitors perused OPSWAT's purpose-built advanced technologies, its experts celebrated Cybersecurity Awareness Month by offering complimentary CIP certifications to attendees at the company's event stand

and through on-demand sessions. "This OPSWAT Academy initiative not only enhanced the GITEX learning experience for participants but reinforced our commitment to advancing cybersecurity knowledge and skills across the industry," commented Irfan Shakeel, VP of Training and Certification Services at OPSWAT.

As part of Cybersecurity Awareness Month, the OPSWAT Academy also ran a Cyber Challenge, where participants enhanced their skills while having the chance to win prizes. Additionally, there were quizzes designed to test and expand visitors' understanding of cybersecurity fundamentals.

Alongside the competitions and training, OPSWAT actively engaged with IT professionals and key stakeholders at GITEX. "We aimed to build and strengthen strategic partnerships that enhanced cybersecurity integration across diverse technological domains," Selcuk explained. "Our focus was on creating collaborative opportunities that addressed both IT and OT security challenges, driving innovation and enhancing our collective ability to protect that which matters most from that which threatens us most."

At GITEX Global 2024, OPSWAT exhibited at the "CyberValley" section – Stand H25-C70, Hall 25.



VECTRA AI:TACKLING IDENTITY BREACHES AND ADOPTING CLOUD SECURITY INNOVATION

VERONICA MARTIN CAUGHT UP WITH TAJ EL-KHAYAT, AREA VICE PRESIDENT - SOUTH EUROPE, MIDDLE EAST, TURKEY AND AFRICA (SEMEA) AT VECTRA AI TO DISCUSS THE KEY PRODUCTS AND SOLUTIONS THEY ARE SHOWCASING, HOW THE COMPANY IS LEVERAGING AI TO ENHANCE THEIR OWN PRODUCT PORTFOLIO AND THEIR UPCOMING TRENDS FOR 2025.

an you outline to our readers what your company's focus and theme is at this year's GITEX 2024 - and what key products and solutions are you showcasing at your stand?

One of our key focuses at GITEX this year is our Al-driven threat detection and response platform, which continues to evolve with more attack surface coverage and sophisticated behavioural detections. We aim to protect organisations from zero-day and unknown threats. This year, we're emphasising three main areas:

First, we're addressing the rise in identity breaches. Hackers aren't hacking—they're logging in. Our mission is to protect organisational identities by focusing on both pre- and postlogin activities, leveraging AI to detect malicious behaviour in identity-centric attacks.

Second, we've launched a Managed

Security Services (MSSP) partner program. In previous years, GITEX was all about technology. This year, we're focusing on what's in it for our partners—enabling them to monetise our solutions and strengthen relationships with their customers. We're making it easier for MSSPs to acquire licensing, reducing pricing complexity, and streamlining onboarding.

Third, we've introduced our Respond UX (RUX) platform, bringing the power of our on-prem AI platform to the cloud. This SaaS offering makes it easier for organisations to adopt AI-driven security solutions without the infrastructure burden, offering speed, scale, and simplicity for both large enterprises and those with limited capabilities.

Our focus is on identity security, empowering partners, and offering flexible, scalable Al solutions across on-prem, air-gapped, and SaaS environments.

The central theme of GITEX 2024 is Al. Can you provide our readers with a better understanding of how your company is leveraging Al to enhance your own product portfolio that is ultimately designed to deliver better outcomes for your customers?

I'm not sure if this is perceived as good or bad, but we've been doing this for 13 years. When we first decided to integrate Al into cybersecurity, many thought we were crazy. People asked, "Isn't Al insecure? How can it protect against cyber threats?" Fast forward to today, and Vectra has become synonymous with Al-driven cybersecurity. Recently, we were honoured with Gartner's Customer Choice Award for 2024, the only cybersecurity company to receive this recognition. This is something we take immense pride in because it's a reflection of customer feedback—a rating system that we can't influence. It's a true testament to the value we bring to our clients.

At the core of what we do is a commitment to empowering organisations to enhance their security operations and make the world a safer place using Al. That's our North Star. How do we achieve this? By leveraging Al to support security analysts. Our Al reduces their workload, minimises burnout, and allows them to focus on high-priority threats instead of overwhelming, low-level tasks. This not only improves their longevity in the role but also allows them to transition from generalists to specialists in Al security, opening new career paths.

Our AI handles threat detection, triaging, and prioritisation, eliminating the need for analysts to search for the proverbial needle in a haystack. This significantly improves efficiency in security operation centres and ensures human analysts can focus on what really matters.

As for our broader mission, we're committed to using AI for good. As the rise of generative AI brings new malicious threats, we're focusing on developing AI that combats those risks—AI fighting AI. Additionally, we leverage AI internally for capacity planning, forecasting, and partner support, simplifying our operations while driving success in the market.

Ultimately, we aim to protect the critical sectors of society—healthcare, education, and banking—from zero-day attacks. Our mission is to ensure that these vital industries are safeguarded against evolving threats, contributing to a fairer, safer world for everyone.

The opportunities of Generative AI are boundless. However, there are valid ethical and data privacy concerns in relation to Gen AI. How important is it for robust regulations and frameworks to be established in order to safely accelerate the deployment of Gen AI across the enterprise space?

Here's how I see it: think back to when cloud computing first emerged.

People were hesitant, asking, "How can I let my data be stored somewhere I can't control?" Even today, there are still some uncertainties. But over time, companies realised that if they wanted to grow, expand, and scale, they needed the power of cloud infrastructure—something that offers speed and scalability. They understood that avoiding the cloud would limit their growth, so regulations were put in place to protect data.

The same is happening now with generative AI. Gen AI is here to stay, and it will become a major part of our lives. Look at examples like Microsoft's Copilot. You're writing an email, and a suggestion pops up to enhance your writing—that's AI at work. Or when banks use facial recognition for transactions, that's AI too. These systems are already regulated. For instance, banks and consumer tech companies like Microsoft follow strict guidelines to ensure AI is used responsibly.

As generative AI becomes more sophisticated, I believe governments will step in with regulations, similar to GDPR, that define not just how AI can be used but also how it's trained. Stricter guidelines will emerge around both the development and application of AI technologies.

From a security perspective, organisations will also put measures in place to limit AI's misuse, preventing it from becoming a gateway for cyber threats. We'll see more protective AI tools—Vectra is already a leader in this space—but many other companies are focusing on AI-driven cybersecurity.

Ultimately, just like cloud computing and data privacy, AI will be regulated—and likely much faster. The companies that adopt AI will need to ensure they have the right policies in place to use it safely and effectively, so it doesn't turn into a liability.

Outside of AI, what other trends do you see emerging across the technology

landscape in 2025?

From what's happening here in the region but also from events we've attended across Europe and the U.S., cloud computing, while not new, will continue to play a critical role in AI. Today, some of the biggest global companies are partnering with major cloud providers to prepare the infrastructure needed for AI's growth. AI requires immense processing power—GPUs, LPUs—and this kind of scale and capacity can only be achieved through the cloud. So, cloud computing remains crucial for deploying AI effectively.

The second factor is the rise of IoT, which will expand as AI integrates more with robotics. Robotics will essentially function as part of the Internet of Things, and to manage and orchestrate these systems, cloud infrastructure will again be key to supporting this growth.

Another major enabler will be the deployment of 5G networks. 5G will drive a new wave of smart city adoption, and even beyond that, we'll see the emergence of cognitive cities. Though 5G has been in discussion for years, the high costs and lack of readiness have slowed widespread adoption. But as technology evolves and costs become more manageable, 5G will become a catalyst for this transformation.

Lastly, cybersecurity will remain a top priority, with significant investments being made in advanced security measures. Al is part of this, but we'll also see innovation aimed at addressing the current skills shortage in cybersecurity. Automation, robotics, and predictive technologies will help quide less experienced analysts by providing actionable insights—moving from "mean time to detect" and "mean time to respond" to "mean time to solve." As we rely more on machines and AI, cybersecurity risks will increase, making ongoing innovation in this space essential to protect organisations. 1



06 - 08 MAY 2025 **DUBAL WORLD TRADE CENTRE**

HOSTED BY



OFFICIAL GOVERNMENT CYBERSECURITY









MIDDLE EAST AND **AFRICA'S LARGEST** CYBERSECURITY EVEN

SCAN HERE



ENQUIRE FOR 2025!





















GOLD SPONSORS

kaspersky











SILVER SPONSOR ·I!I·Recorded Future®

CONTACT

⊠ gisec@dwtc.com

emt \$9

+971 4 308 6469



#gisecglobal



HIKVISION LEADS THE WAY IN COMMERCIAL DISPLAY TECHNOLOGY

THE COMPANY SHOWCASED IMPRESSIVE FLEXIBLE LED DISPLAYS AND IOT-DRIVEN SOLUTIONS AT GITEX.

t GITEX, Hikvision took centre stage to redefine its market perception. While traditionally recognized as a CCTV powerhouse, the company showcased its diverse portfolio as an IoT leader with a strong focus on commercial display solutions. Sachin Srinivasan, Commercial Display Business Director for the Middle East and Africa, gave an insight into the company's latest innovations and future direction in the commercial display market.

He said: "At GITEX, 70% of our solutions on display were focused on commercial displays." The company's presence at the event featured cutting-edge technologies, including flexible LED modules, ultra-bright LED walls, and innovative solutions designed for diverse commercial environments.

Among the highlights was a 1.2-pixel pitch flexible LED module capable of flexing up to 120 degrees, both concave and convex, offering remarkable adaptability for different client requirements. With various pixel pitches such as 1.2, 1.5, 1.8, and 2.5, the company ensured its solutions were tailored to meet viewing distance needs.

A particularly striking display was a 0.7-pixel pitch LED featuring 1000 NITs of brightness, delivering a 4K LED wall at an impressive three meters wide and 1.67 meters high. This installation was integrated with Hikvision's central software and operated in collaboration with Rpg, a company specializing in console solutions. This integration allowed for advanced analytics in control room environments, making Hikvision a comprehensive solution provider.

Hikvision's portfolio included an all-in-one LED wall, presented at GITEX as a 108-inch screen with a 1.2-pixel pitch. This display, enhanced with Hikvision's glue-on-board (HOB) technology, boasted an IP65 rating for improved durability and contrast and a matte finish for superior visual clarity. The all-in-one design incorporated an LED controller, digital signage box, Windows PC, wireless sharing capabilities, and 2.1 surround



sound. It could be wall-mounted or placed on a stand, offering versatility.

Further extending their innovation, Hikvision developed portable LED posters that could be mounted on walls or placed on trolleys for mobility. With in-house manufacturing and stringent quality control procedures, such as heat dissipation tests and RF testing, the company guaranteed durability and performance across all products.

Hikvision also presented a 3.9-pixel pitch outdoor LED screen designed for seamless 3D content display, with special corner bars eliminating visual lines. The company also offered a 2.6-pixel pitch outdoor LED rental screen, an increasingly popular choice among event organizers due to its quality and ease of use.

Latest trends

When asked about the latest trends, Srinivasan highlighted the increasing prominence of flip-chip COB (Chip-on-Board) technology in the commercial display market. This innovation, he explained, had the potential to eclipse LCD technology, especially with pixel pitches as low as 0.7, 0.9, and 1.2. Hikvision was

WE BELIEVED THE

FUTURE OF DISPLAY

TECHNOLOGY WOULD

EVOLVE TO 0.1-PIXEL

PITCH.

actively developing a 0.5-pixel pitch display.

"We believed the future of display technology would evolve to 0.1-pixel pitch," he said. "While the production costs of flipchip COB were currently high, we expected them to decrease, driving demand and ultimately leading to the phase-out of LCD technology in the next four to five years."

Another growing trend was the demand for interactive displays, particularly within meeting rooms and education verticals. Hikvision was at the forefront of this trend with interactive displays that offered Android operating systems and access to the Google Play Store, unlocking a wide range of third-party applications.

For instance, Hikvision's digital signage screens operated on Android OS, allowing integration with various software providers. Interactive displays could host Google management services, opening up vast possibilities for customization. Hikvision's LED displays also came with proprietary video controllers, but clients could also use third-party options.

Hikvision's future plans included the launch of new flip-chip COB LEDs with a 0.6-pixel pitch and continued innovation in developing custom LEDs for creative applications. In the realm of interactive displays, the company focused on enhancing compatibility with third-party software, particularly for education environments.

"We continually pushed the envelope with creative and customizable LED solutions," Srinivasan concluded. "When you thought of the future of vision technology, think Hikvision."

AHAD'S HIGHLIGHTS CYBERSECURITY

INNOVATIONS, RISK MANAGEMENT, AND AI-DRIVEN DIGITAL TRANSFORMATION

EMPOWERING THE FUTURE WITH AHAD'S CYBER RESILIENCE AND DIGITAL TRANSFORMATION INNOVATIONS



uneeb Anjum, CEO of AHAD, alongside Somnath Sarkar, CISO, delve into AHAD's cutting-edge advancements in cybersecurity, digital transformation, and risk management. The duo outline the strategic deployment of AHAD's Security Operations Center (SOC) services across the UAE and Saudi Arabia, which are tailored to meet stringent data privacy laws and enhance cyber resilience.

AHAD is integrating artificial intelligence to revolutionize digital transformation efforts, creating personalized Al-driven solutions that empower organizations across various sectors.

Muneeb Anjum, CEO, AHAD and Somnath Sarkar, CISO, AHAD discuss the company's advanced cybersecurity solutions and verticals in digital transformation and risk management.

Q: Can you discuss the recent innovations AHAD has introduced to enhance cyber resilience and business efficiency?

Muneeb: Certainly! AHAD has recently launched our own Security Operations Center (SOC) services in the UAE and Saudi Arabia. This service offers comprehensive managed detection

and response capabilities suitable for organizations of any size, from Fortune 100 companies to startups. Particularly relevant are the data privacy laws in regions like Saudi Arabia, the UAE, Oman, and Egypt, which require organizations to respond within 72 hours in the event of a breach. Our SOC services are designed to meet these stringent requirements, enhancing both cyber resilience and compliance with local laws.

Q: How is AHAD leveraging emerging technologies to help organizations navigate the challenges of digital transformation?

Muneeb: AHAD is at the forefront of integrating artificial intelligence into digital transformation strategies. We're working closely with public sectors, private organizations, and large enterprises to harness Al's capabilities. Our focus includes developing personalized use cases ranging from Al agents that perform specific tasks to complex workflows that manage vast amounts of data. For example, we are integrating voice agents that can instantly respond to gueries, which is a part of our effort to combine human and machine capabilities. This integration is leading what we see as the next revolution in technology, aiming to empower organizations through the effective use of Al in their digital transformation journeys.

Q: Can you provide an overview of AHAD's core services in cybersecurity, digital transformation, and risk management?

Somnath: Absolutely. At AHAD, we focus on three primary verticals. First, in cybersecurity, we concentrate on proactive cyber defense through our



cyber defense centers located in three different geographies. Our approach here is mostly offensive, involving red teaming exercises, penetration tests, and robust cyber defense services. The second vertical is digital transformation, where we manage comprehensive transformations across people, processes, and technology for companies, aligning these with business strategies to enable digital empowerment. Lastly, our risk management services focus on comprehensive risk assessments, enhancing cyber and operational resilience, and facilitating ISO and NIST certifications to prepare organizations for the latest technologies.

OUR FOCUS INCLUDES DEVELOPING PERSONALIZED

USE CASES RANGING FROM AI AGENTS THAT PERFORM SPECIFIC TASKS TO COMPLEX WORKFLOWS THAT MANAGE VAST AMOUNTS OF DATA.

Q: How does AHAD tailor its cybersecurity solutions for government bodies, Fortune 500 companies, and startups?

Somnath: Our cybersecurity strategies are tailored to the specific needs of different types of organizations. For government bodies, we focus on national and state-level security, managing regulations, and ensuring comprehensive access and credentials management. For Fortune 500 companies, which operate across multiple geographies, our emphasis is on cross-border data transfer compliance and a cohesive global cybersecurity framework that addresses various international standards. In contrast, for fintechs and startups, our approach is more nimble and cost-effective, offering modular solutions that can scale with the business. These solutions are designed to be light yet robust enough to provide essential protection at a lower cost, fitting the unique needs of smaller, dynamic companies. 🙎



AMISEQ LEVERAGES EXPERTISE AND PARTNERSHIPS TO DELIVER COMPREHENSIVE CYBERSECURITY SOLUTIONS

SECURING TOMORROW WITH AMISEQ'S EXPERT SOLUTIONS FOR TODAY'S CYBERSECURITY CHALLENGES

hahnawaz (Shah) Sheikh, VP – Global Sales & Alliances (Cybersecurity Practice), Amiseq and Moiz Ghadiali – Director Global Delivery, Amiseq, shared that AMISEQ brings cuttingedge cybersecurity solutions through skilled expertise, vendor-agnostic services, and a global delivery team, ensuring lasting value for customers and partners.

What is Amiseq's go-to-market model, and do you sell your services directly or via channel partners?

Shahnawaz: AMISEQ has multiple business practices, namely Intelligent Automation, Product Engineering, Cloud and Cybersecurity. Within Cybersecurity practice, we deliver Incognito services which is a white labelled services to several cybersecurity vendors and secondly Fusion services which are vendor agnostic services. Our Go-to-market approach is to offer these services via vendors and/or channel partners.

What do you expect from an event like Gitex? Are you looking at new partnerships?

Shahnawaz: From event like Gitex, we get an opportunity to connect with some of our existing vendors and their leadership teams from EMEA or US, secondly an opportunity to connect with prospective vendors for new partnerships. Been a neutral professional services company, we also engage with multiple distributors and partners in the region and deliver white labelled services to them. We have also experienced at Gitex that customers these days not just give importance to products and technologies but also seek for Cybersecurity services companies to help them with consulting and deployment.

Why Amiseq? What are the key differentiators you offer to your customers and vendors?

Shahnawaz: AMISEQ been a focused services company we strongly believe that we can present a competitive value to our vendors and partners by bringing in skilled expertise with hands-on experience and certifications to carry out the work. Additionally, we have built our own IP's as accelerators that help in speedy deployments, automated health checks, some custom scripts to solve integration or interoperability challenges and a test lab for such integration test to be carried out before been applied in customers production environment. Good understanding of the region and its human resource logistics requirements, security clearance to serve sensitive government entities and a global delivery team are some added advantages.

How do you deliver the white labelled services and what are the skills and capabilities Amiseq possess?

Moiz: Our technical team brings a wealth of experience across various cybersecurity technologies, enabling us to quickly adapt to new tools and understand their complexities. We follow a structured process where all engineers first achieve the necessary certifications and are then screened by experts from the vendor side to ensure they meet the required standards to work on projects.

Following certification, engineers shadow at least one project to learn best practices directly from the vendor's technical team. In the next phase, our Amiseq engineer leads a project with vendor technical personnel overseeing the deployment to confirm all aspects are mastered. Once these steps are successfully completed,

Amiseq consultants are fully prepared to independently deliver projects, while adhering to high standards and vendorapproved methodologies. Our team is well-trained and certified to handle deployments across a broad range of technologies, including SIEM, Vulnerability Management, EDR, Identity Solutions, Data Classification, Unified Endpoint Management, XDR, Network Security, and more.

What are Fusion services from Amiseq, how are your customers going to benefit from such services and see a value in such offering?

Moiz: Amiseq Fusion Services offer comprehensive support to a diverse range of partners and customers, addressing cybersecurity needs across various industries. These services are tailored to meet different security requirements, from assessing an organization's initial security posture to providing ongoing threat detection and incident response. This extensive suite of services allows Amiseq to establish lasting relationships with customers and partners, providing them with targeted support at each stage of their cybersecurity journey.

Amiseg Fusion Services help organizations enhance cybersecurity practices, optimize operations, and build resilience against evolving cyber threats. By offering services such as Vulnerability Assessment and Penetration Testing (VAPT), Data Governance, Cybersecurity Gap Analysis, Incident Response and Forensics, and Identity and Access Management (IAM), Amiseg ensures that customers and partners have access to comprehensive cybersecurity solutions. Additionally, advanced services like Red, Blue, and Purple Teaming, Application Security, and OT (Operational Technology) Security further support customers in managing complex security challenges.

With this range of capabilities, Amiseq Fusion Services empower customers to proactively manage cybersecurity risks, while partners benefit from specialised training and resources that enhance their ability to support clients effectively.

CUSTOMERS THESE DAYS NOT JUST GIVE IMPORTANCE

TO PRODUCTS AND TECHNOLOGIES BUT ALSO SEEK
FOR CYBERSECURITY SERVICES COMPANIES TO HELP
THEM WITH CONSULTING AND DEPLOYMENT.

5G ADVANCED: THE INVISIBLE UPGRADE THAT COULD TRANSFORM DAILY LIFE

akesh Lakhani, Head of Networks Solutions, Ericsson Middle East and Africa, highlights the unique capabilities of 5G Advanced, from enhanced network reliability and Al-driven automation to groundbreaking outdoor positioning and energy efficiency—innovations that promise to reshape connectivity for both individuals and industries alike.

When 5G first arrived, it was advertised as a revolution in connectivity, promising blazing speeds and instant data access. But for most of us, the experience has been more evolutionary than revolutionary. At face value, videos load faster, and downloads complete in

seconds, but the promised transformative impact has felt out of reach, especially for people who aren't directly involved in tech or industry. Now, however, we're on the brink of a more significant upgrade: 5G Advanced. This new phase has the power to do more than just improve personal device speeds; it aims to make networks smarter, more efficient and more responsive to real-world needs in ways that could impact everyone. In other words we are progressing towards Programmable Networks.

With 5G Advanced, Ericsson is pushing beyond the basic improvements in speed and capacity to create a network that can handle the complexity of our connected world. We are targeting highperforming programmable networks with new 5G Advanced products. Our recent advancements are designed to meet the challenges that current 5G networks struggle with, from energy consumption to service reliability and Artificial Intelligence (AI) Automation. While these upgrades might seem technical, their potential to shape everyday life is enormous. Real-world benefits, like more accessible healthcare, improved public safety, reduced environmental impact and longer-lasting devices, could all become possible.

One of the most noticeable changes 5G Advanced will bring is more reliable network performance, especially during heavy use. Real-time AI-powered



automation automatically monitors and manages the network, responding to demand changes and optimising performance on the fly. This, along with radio access network (RAN) differentiated connectivity, which allows networks to manage multiple services at once while maintaining quality for each, will provide much smoother and more reliable connectivity for everyone during busy periods. Where a normal 5G network may struggle with a stadium full of people posting and streaming, 5G Advanced is equipped to handle the massive uptick of bandwidth demand without compromise. That where premium network performance and advanced performance features enable more coverage and

capacity in the most traffic-loaded scenarios.

Another groundbreaking benefit of 5G Advanced is outdoor positioning. This allows providers and enterprises to introduce location-based services with or without GPS using 5G standalone architecture, which can fill in the gaps of GPS and provide reliable and accurate location services. For example, it can support continuing navigation in tunnels, where it would otherwise falter, enabling emergency services to quickly pinpoint people in distress, or allow courier companies to keep track of their packages and streamline logistics. It can make people's lives not only easier but safer as well.

For sectors whose connectivity is paramount, Ericsson's mission-critical services technology ensures they can continue to operate during extreme conditions. With 5G Advanced, critical services – such as emergency response systems, defence communications and railway signalling – can remain fully operational in any environment. In practical terms, this means first responders will have uninterrupted communication during natural disasters or large-scale events, when demand on infrastructure is high. By supporting these essential services. 5G Advanced makes cities and communities safer and more resilient in times of crisis.

Finally, 5G Advanced products also increases energy efficiency for both the infrastructure and consumer devices by optimizing power use across the network while reducing costs and environmental impact, which is a win for everyone. On the consumer side, 5G Advanced requires less powerhungry devices. With the device battery performance, it allows service providers to enhance the battery performance of any 5G device, including smartphones, wearables and AR/VR glasses with intelligent network features that save battery power.

All together, these seven innovations we have developed highlight the broader purpose of 5G Advanced. This isn't just a technology upgrade for industries; it's a leap towards smarter, more resilient programmable networks that can support real-world needs in ways that benefit everyone. The true success of 5G Advanced won't be measured by download speeds but by the way it enhances the quality of everyday life, from better public services to a more sustainable environment.

As 5G Advanced rolls out, the conversation around 5G should shift from faster internet to resilient vital infrastructure. At Ericsson, we can lay the foundation for these improvements, but it's up to industries to build upon it 1

BUILDING A CYBERSECURITY FRAMEWORK CAN ALIGN SECURITY FUNCTION WITH BUSINESS AND MAKE IT FUTURE-READY

GROWING BUSINESS IMPORTANCE OF THE CYBERSECURITY FUNCTION COUPLED WITH SOPHISTICATION OF EXTERNAL CHALLENGES AND INTERNAL COMPLEXITY IS PUTTING PRESSURE ON CYBERSECURITY DECISION MAKERS. RANJITH KAIPPADA, MANAGING DIRECTOR OF CLOUD BOX TECHNOLOGIES DESCRIBES HOW A CYBERSECURITY FRAMEWORK CAN HELP ALL EVIATE MUCH OF THESE PAINS.

arge scale adoption of digital and business transformation by global and regional enterprises and the associated cybersecurity vulnerabilities, has driven the realization of the importance of keeping cybersecurity at the same levels as other strategic priorities of the enterprise.

According to IDC, security is now a board-level conversation and cyber risk has been elevated and is now recognized as a business risk. According to Gartner, importance of information security is rising rapidly as senior executives become aware that poor security can cause irreparable damage to the business. Gartner forecasts that by 2026, 70% of boards will include one member with cybersecurity experience.

However, this rapid onslaught of digital transformation with migration to the cloud and adoption of digital platforms, followed by the more recent drive to embed Generative Al into business processes is not making things easier for cybersecurity administrators and decision makers.

Complex challenges for CISOs

The continued heightened threat environment, cloud migration and talent crunch are pushing security to the top of the priorities list and pressing cybersecurity administrators and decision makers to increase their organization's security spending.

As organizations continue to move to the cloud, Gartner analysts expect an increase in cloud security solutions, and the market share of cloud-native solutions will grow.

In reality, the emergence of Generative AI and other AI technologies are contributing to increased budgets for security offerings in 2024. Generative AI is driving an increase in cybersecurity spending to secure an organization's development and use of Generative AI applications, as well as to use Generative

All assistants to support security administrators in efficiency.

Adoption of Al and Generative Al continues to drive an increase in the investments in security software like application security, data security and privacy, and infrastructure protection. Generative Al will trigger a spike in the cybersecurity resources required to secure it, leading to an expected 15% increase on security software spending, forecasts Gartner.

Furthermore, organizations are currently assessing their endpoint protection platform and endpoint detection and response needs, and adjusting to boost operational resilience and incident response following the CrowdStrike outage.

Since the release of Generative AI, attackers are increasingly employing tools along with large language models to carry out large-scale social engineering attacks. Gartner predicts that by 2027, 17% of total cyberattacks and data leaks will involve Generative AI.



Security spending will continue to remain strong and isolated from the recessive effects of a challenging macro-economic global environment and economic uncertainty.

Developing a cybersecurity framework

The way forward for cybersecurity administrators and decision makers is to build a forward-looking cybersecurity framework that manages continuous digital and business transformation, helps to create new business value in the face of these changes, takes into consideration internal and external factors, and plans for growing risks and threats

In the absence of such a forward-looking cybersecurity framework, the role of cybersecurity administrators and cybersecurity decision makers may be relegated to merely managing technology solutions and technology implementations. This may have little relevance to the business of the enterprise, its position in global and regional markets, and its changing business value in the competitive market place.

A well thought and planned out cybersecurity framework has multiple components. These can be listed as:

- Overall strategy
- Collection of operational processes
- Accountability and governance
- Correlation to the rest of the enterprise
- Mandate for operational execution

A fully functional enterprise cybersecurity framework consists of security policies, security processes and security architectures. It defines users, systems and configurations. It provides guidance for future design, implementations and successful operations.

A well-developed enterprise cybersecurity framework allows for future evolution and is adaptive to changes in the threat landscape. This exercise cannot be completed in a hurry and must be well mapped to the business organization of the enterprise.

Developing this framework is a team effort from across the enterprise and involves business decisions makers whose presence helps to collectively shoulder the risk and governance across the enterprise.

Cross functional involvement

A successful and fully operational enterprise cybersecurity framework requires a cross functional team, building it up from infancy to reach on-going operational maturity that can help steer the enterprise through future cybersecurity threats and growing sophistication in malware attacks.

The following teams have a role in building the enterprise cybersecurity framework:

Cybersecurity Decision Maker

This executive, usually the CISO, is the mainstay and champion of an enterprise cybersecurity framework. This executive along with the rest of the cybersecurity team leads the development of the framework and ensures there is alignment with the business objectives of the enterprise.

This executive collaborates with peers and other decision makers to facilitate its adoption. This executive also communicates the implementation progress to the management and other stakeholders.

IT Decision Maker

This executive, usually the CIO, supports the CISO in building the framework, alignment with business objectives of the enterprise, and communication of the progress to stakeholders.

Innovation Experts

They work with the CISO, business heads, and other stakeholders to understand and consolidate the cybersecurity requirements of the enterprise into the enterprise cybersecurity framework.

Domain Experts and Architects

This team assesses the operational



skills and technology readiness of the enterprise's business to implement security policies and governance. They are also responsible for cybersecurity training and for building cybersecurity skills.

Infrastructure Leader

This executive and the team assists the CISO with implementation and operations of key components of the enterprise cybersecurity framework.

Software Engineers

They are responsible for implementation of the enterprise cybersecurity framework and its regular operations. Typically they would be using DevSecOps in software development to support the enterprise framework.

Strategy Leader

This executive leverages partnerships for coordination, delivery, risk mitigation, and organizational change during implementation of the enterprise cybersecurity framework to ensure project completion.



Building the cybersecurity framework

This is a step by step process and successful completion and operational launch of the enterprise cybersecurity framework requires rigorously going through the following steps.

#1 Planning

The first stage begins by defining the business priorities of the enterprise and an assessment of the cybersecurity drivers and threats. The mission of the enterprise cybersecurity framework is stated as well as the goals, the value to be generated, and roles and responsibilities of stakeholders involved.

#2 Assessment

The second stage begins with the road map that has been prepared from the first stage. Existing systems, technologies, people, processes, third parties are assessed and a security audit completed. This stage maps the journey through the intermediate stages to the final stage and completes the gap analysis between the stages.

#3 Development

By the third stage the documentation for

the enterprise cybersecurity framework has been completed and is now the basis for forward implementation. The documentation defines tools and technologies to be utilized, composition of the team with roles and responsibilities, escalation process to stakeholders, minimum cybersecurity competencies required in the enterprise and a training program to fill the gaps in cybersecurity skills.

#4 Buy-in

The fourth stage is critical for the future roll out of the enterprise cybersecurity framework. In this stage there is an outreach campaign to the decision makers within the enterprise showcasing the value being delivered by the enterprise cybersecurity framework.

This helps to build top-down support for the cybersecurity framework and to achieve representation within the Board. Another objective of the outreach campaign is raise awareness of security best practices amongst employees and the importance of developing a healthy security culture.

#5 Robustness

Unless the enterprise cybersecurity framework is robust enough to continuously improve itself against future threats and changes to the enterprise, its usage will soon run out of momentum.

Amongst the forward looking steps is to build competency in reverse engineering of threats, determination of threat origins, monitoring of advanced threats, enterprise wide incident response capabilities, and action plans for employees in the face of threat actor intrusions.

It is not of much use to build an ambitious enterprise cybersecurity framework and not have measures to accurately benchmark its usefulness and improve its functioning, so that it can continuously support the enterprise as it transforms its business value and purpose in the future. And this is the purpose of the final stage.

By following the above steps cybersecurity decision makers can help the security function align with business and also showcase the importance of its role and the value it can offer today and in the future as well.

MIDDLE EASTERN FIRMS SURPASS EUROPEAN COUNTERPARTS IN CYBERSECURITY, SAYS REPORT BY SECURITYSCORECARD

he Middle East has
emerged as a frontrunner,
outperforming European
companies in safeguarding
digital assets, according to a
new report by SecurityScorecard.

This comprehensive analysis, conducted in partnership with CyberKnight in the UAE, unveils critical insights into the cybersecurity posture of the top 100 Middle Eastern companies by market capitalization, revealing a significant edge over their European counterparts in several key areas.

The Cybersecurity Divide: Middle East vs. Europe

The report's findings are both revealing and encouraging for the Middle Eastern market. Notably, only 2% of these companies experienced a direct cyber breach in the past year—a stark contrast to the 18% in Europe and 21% among S&P 500 companies. This data not only highlights the effectiveness of Middle Eastern cybersecurity strategies but also underscores the ongoing vulnerabilities in European markets.

Sector-Specific Insights and Challenges

The sectoral breakdown within the report provides a nuanced understanding of the region's cybersecurity landscape:

- Utilities: Emerge as the most secure sector, with no companies scoring below a C rating and no direct breaches, setting a benchmark for others.
- Energy: Shows resilience with only 7% of companies rated C or lower,





compared to a concerning 75% in Europe.

 Telecommunications: Identified as the most vulnerable, with a high 86% of companies scoring C or lower, signaling an urgent need for enhanced security measures.

These disparities in sector performance illustrate the varied challenges industries face and the critical need for tailored cybersecurity strategies.

Third-Party Risks: A Persistent Threat

Despite strong overall performance, third-party breaches remain a significant concern, with 84% of Middle Eastern companies affected. This is still notably lower than Europe's 98%, reflecting more robust third-party risk management but also highlighting the pervasive challenge of securing extended enterprise environments.

The Role of Cyber Risk Ratings

SecurityScorecard's report advocates for the adoption of cyber risk ratings, akin to credit ratings, to standardize cybersecurity

resilience. Companies in the Middle East with higher ratings consistently reported fewer breaches, validating the effectiveness of proactive security measures. Jeff Le, VP of Global Government Affairs & Public Policy at SecurityScorecard, emphasized the importance of these ratings:

"The Middle East's energy and financial sectors are linchpins of the global economy, underscoring the urgent need for robust cybersecurity measures. Our data clearly shows that organizations with top-tier cybersecurity ratings are far less likely to experience breaches."

The Impact of Global Cybersecurity Standards

With upcoming regulations like the Digital Operational Resilience Act (DORA) and the NIS2 directive in the European Union, the report highlights the importance of harmonized cybersecurity standards. These regulations aim to enhance the resilience of network and information systems within the EU, offering a framework that could benefit

global cybersecurity practices.

SecurityScorecard's Methodology and Influence

The methodology employed by SecurityScorecard involves non-intrusive, real-time data collection, assessing factors like network security, malware infections, and application security from August 2023 to August 2024. Each company is scored from A to F, with F-rated companies being 13.8 times more likely to suffer a breach.

Since its inception in 2013 by Dr.
Aleksandr Yampolskiy and Sam
Kassoumeh, SecurityScorecard has risen
to prominence by providing essential
cybersecurity benchmarks used by over
25,000 organizations worldwide.

Conclusion: The Path Forward

The report not only sheds light on the current state of cybersecurity in the Middle East compared to Europe but also sets the stage for future improvements. It serves as a call to action for companies worldwide to adopt rigorous cybersecurity measures, invest in continuous monitoring, and engage in proactive third-party risk management to safeguard against evolving cyber threats. As global cyber risks continue to rise, the insights provided by SecurityScorecard offer valuable guidance for strengthening cyber defenses and building more resilient digital ecosystems.

SECURITYSCORECARD'S LATEST ANALYSIS

HIGHLIGHTS SUPERIOR CYBERSECURITY
MEASURES AMONG TOP MIDDLE EASTERN
COMPANIES COMPARED TO EUROPE, EMPHASIZING
STRONGER DEFENSES AND FEWER BREACHES.

MIDDLE EAST RETAILERS **INCREASINGLY VIGILANT OF EMAIL** FRAUD RISKS AND TAKING STEPS TO SAFEGUARD SHOPPERS

90% OF TOP MIDDLE EAST RETAILERS HAVE PUBLISHED A DMARC RECORD, REFLECTING IMPROVED EMAIL SECURITY MEASURES



s the holiday and shopping season approaches, leading cybersecurity and compliance company Proofpoint has released research that shows that the top Middle East retailers are steadily improving their email security measures, better protecting customers from the potential risk of email fraud.

These findings are based on a Domainbased Message Authentication, Reporting, and Conformance (DMARC) adoption analysis of the top retailers in the Middle East. DMARC is an email authentication protocol designed to protect domain names from misuse by cyber criminals. It authenticates the sender's identity

before allowing a message to reach its destination. DMARC offers three levels of protection: monitoring, guarantine, and rejection, with rejection being the safest way to prevent suspicious messages from reaching the inbox.

The analysis reveals that a vast majority of Middle East retailers (90%) have published a DMARC record, and 8 out of the top 20 (40%) have the strictest and recommended DMARC policy ('reject') in place. This is a slight improvement from last year - where findings suggested that only 30% had implemented the DMARC policy at 'reject' level and were proactively blocking fraudulent emails from reaching consumers.

According to a study by IMARC, the Middle East retail market size is projected to grow by 4.21% from 2024-2032, driven by a surge in population and evolving consumer preference for online shopping. Through the high traffic of retail activity, attackers are now using new tactics to exploit their human targets.

Emile Abou Saleh, Regional Director, Middle East & Africa at Proofpoint, said: "Middle East retailers realize the risks millions of consumers face daily when they shop online. Our research shows that phishing, ransomware, and business email compromise remain among the top attack vectors plaguing organizations across all industries. Amid a surge in e-commerce in the region, deploying authentication protocols, such as DMARC, will be critical to support the growth and security posture of the retail sector."

Email remains the number one threat vector, and phishing emails can lead to unsafe websites that gather personal data, such as credentials and credit card data. Therefore, it is always best to go directly to the source of the advertised deal by typing a known website address directly into a browser. For special offer codes, Proofpoint recommends entering them at the checkout to see if they are legitimate. It also recommends using a password manager to make the online experience seamless, whilst staying safe and using a multi-factor authentication for an added layer of security. 1



Bye-bye blind spots.

Pan-Tilt Indoor Camera

Discover our first Security Camera to offer 360° pan and 169° tilt coverage of every room, controlled by your phone. With Pan-Tilt Indoor Camera, you can adjust the angle to check-in on your kids or pets, all from the Ring app.











Live View & Two-Way Talk



Manual Audio & Video Privacy Cover



HD Video & Colour Night Visior



Plug-In Power



Pets Camera















D-Link®



Experience Next-Generation 5G Connectivity

5G features unparalleled broadband speeds, low latency, increased bandwidth, wide connectivity compared to 4G network, brings new capabilities to indoor spaces.







Higher Speed

Lower Latency

Larger Capacity

Plug & Play, Enjoy Fast Connectivity Where You Need



Easy Setup & Manage









5G NR AX3000 Wi-Fi 6 Router

Dive into ultra-fast connectivity with 5G NSA mode, offering speeds up to 3.4 Gbps*. The G530 5G NR AX3000 Wi-Fi 6 router ensures you enjoy low-latency, high-speed Internet on both 2.4 GHz and 5 GHz bands, perfect for reliable home entertainment and efficient work.

*The theoretical coverage in D-Link Lab testing may vary in different environments.