ISSUE 87 | SEPTEMBER 2024

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST

SECURING THE FUTURE

MANDAR PATIL, SVP-META SAARC & ASEAN AT CYBLE TELLS ANITA JOSEPH HOW AN INTELLIGENT APPROACH TO THREAT DETECTION IS HELPING THE COMPANY SECURE THE DIGITAL FUTURE OF BUSINESSES IN THE REGION.

tahawultech.com

cnme computer news middle east SUPPLEMENT

HIKVISION

EMBRACE AIoT FOR SAFER, SMARTER AND GREENER MOBILITY

Spot danger, stop risk

Detect and respond to incidents swiftly with advanced AI technology.

Streamlined Road Operation

CONTENTS

DGS-F3700 Series

Optimize Your Network

with High-Bandwidth 12, 16, or 20
Port Industrial Managed Layer-3 Gigabit PoE Switch

Powerful PoE

Flexible and cost-effective, this is an ideal industrial solution where high-throughput and high-reliability are fundamental. Especially with NEMA TS-2 Certification, this series is the perfect choice for Smart City and Traffic Control applications.

✦ **Versatile Connectivity**

✦ **Advanced Switching**

✦ **Reliable Redundancy**

D-Link®

EDITOR'S NOTE

Talk to us:
E-mail:
*anita.joseph@
cpimediagroup.com*

Anita Joseph
Editor

CYBERSECURITY LEADERSHIP EXCELLENCE

In today's rapidly evolving digital landscape, leadership excellence in cybersecurity has never been more critical. The complexity and sophistication of cyber threats are escalating, requiring leaders to go beyond traditional methods and adopt innovative, out-of-the-box strategies to safeguard their organisations.

The cybersecurity realm is no longer just about defending against known threats; it involves anticipating and mitigating risks that have yet to emerge. This shift demands a new breed of leader—one who is not only reactive but proactive, leveraging advanced technologies and creative problem-solving techniques to stay ahead of adversaries. Traditional approaches, while foundational, are increasingly insufficient in the face of dynamic and evolving threats.

INNOVATION-FIRST

Effective cybersecurity leaders must cultivate a culture of innovation within their teams. This involves encouraging unconventional thinking, embracing emerging technologies like artificial intelligence and machine learning, and fostering an environment where creativity and strategic risk-taking are valued. The complexity of today's cyber threats requires a departure from one-size-fits-all solutions to more adaptive, tailored strategies that can anticipate and counteract sophisticated attack vectors.

Moreover, leadership in cybersecurity is about collaboration and continuous learning. Engaging with diverse perspectives—whether through cross-industry partnerships or interdisciplinary teams—can yield fresh insights and novel approaches to threat mitigation.

Cybersecurity leaders must champion an agile mindset, driving their teams to experiment with and adopt new tools and methodologies that can outpace evolving threats.

In essence, the future of cybersecurity hinges on leaders who are not only skilled in traditional defense mechanisms but also adept at fostering innovation and adaptability. By prioritising out-of-the-box thinking and embracing cutting-edge technologies, cybersecurity leaders can better protect their organisations against the increasingly complex and multifaceted threats of the digital age.

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by CPI

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

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

EDITORIAL
Editor
Anita Joseph
anita.joseph@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehajan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

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

NEW VEEAM DATA PLATFORM V12.2 EXTENDS #1 DATA RESILIENCE TO MORE PLATFORMS AND APPLICATIONS

Veeam Software, the #1 leader by market share in Data Resilience, announced the release of Veeam Data Platform v12.2, broadening support for protecting data on an extensive range of new platforms while continuing to advance end-to-end cybersecurity capabilities. This latest release combines the most comprehensive data backup, recovery, and security capabilities with the ability to empower customers to migrate and secure data across new platforms. Veeam Data Platform v12.2 is a single, comprehensive solution that provides organisations with the freedom to maintain operational agility and security while safeguarding critical data against evolving cyber threats and unexpected industry changes.

"In a digital world, organisations face three critical challenges: they must protect their data and be able to rapidly recover it no matter what happens; they need the freedom to move to new platforms; and their data must be available where it's needed, including AI," said Anand Eswaran, CEO at Veeam. "At Veeam, we're committed to supporting these critical capabilities for our 550,000 customers, and 12.2 is a major step forward. Veeam Data Platform provides a single platform that delivers data resilience across cloud, on-premises and hybrid platforms bringing together powerful data protection, secure migration, seamless cloud integration, and the industry's most advanced end-to-end ransomware protection. Data is the lifeblood of every organisation and Veeam Data Platform ensures that data is safe, secure and always available."

With Veeam Data Platform v12.2, organisations have the freedom to choose their preferred infrastructure with scalable policy-driven protection. New integration with Nutanix Prism Central provides the best-in-class protection for enterprise needs. Additionally, the new Proxmox VE hypervisor support allows organisations to migrate and modernise on their terms. MongoDB backup is also included, offering immutability, centralised management, and high-speed recovery.

PROVEN ARABIA UNVEILS NEW BRAND IDENTITY; OPENS NEW OFFICE IN RIYADH

PROVEN Arabia, a leading Saudi holding company providing comprehensive solutions, today revealed its new brand identity to showcase its commitment to provide state-of-the-art solutions and services for its customers.

The new brand reinforces the company's aspiration to expand its offerings and enhance its capabilities, ensuring that it remains as a trailblazer in the industry.

"We are proud to highlight our remarkable customers growth both regionally and globally which has inspired our decision to evolve. The expansion of our workforce and the unveiling of our new brand identity, underscores the significant progress we've made over the years. It is also a testament of our hard work and the vision to deliver enhanced quality solutions for our customers. At PROVEN Arabia, we strive to foster a culture built on solid values, continually enhancing our workplace to better serve our team and clients. This new space embodies our dedication to these principles and our vision for the future," said Zaid Al Mashari, Co-Founder and Group CEO PROVEN Arabia.

At the heart of PROVEN Arabia's new identity is an iconic logo that was inspired by a desire to create a visual identity that seamlessly blends both the Arabic and English languages. The modern and sleek design reflects the company's forward-thinking approach, while the fusion of an Arabic version   displays its dedication to inclusivity and cultural roots, thus emphasizing its global outlook and bilingual proficiency.

The brand refresh also includes a new and bigger office space in Riyadh to accommodate their expansion and future growth. The office has an open-space layout, aimed at enhancing communication and collaboration among team members and aligns with the company's commitment to transparency and unity.

By integrating these design elements, PROVEN Arabia aims to create a work environment that not only boosts productivity but also promotes a sense of community and well-being among its employees. Additionally, the new brand encapsulates the company's dedication to excellence, innovation, and customer satisfaction.

AMIVIZ PARTNERS WITH RUNZERO TO DELIVER ENHANCED CYBERSECURITY VISIBILITY ACROSS NETWORKS

AmiViz, the leading cybersecurity- focused value-added distributor headquartered in the Middle East, is proud to announce its strategic partnership with runZero. This collaboration aims to provide unparalleled cybersecurity visibility and exposure management to businesses across the Middle East, further solidifying AmiViz's position as a premier player in the cybersecurity industry.

The runZero Platform is the only comprehensive cyber asset attack surface management solution (CAASM) that uniquely integrates proprietary active scanning, native passive discovery, and API integrations. This powerful combination offers customers the most complete, in-depth security visibility possible, enabling them to mitigate exposures and reduce compliance risks swiftly.

"Partnering with runZero allows AmiViz to offer our clients a state-of-the-art solution that transforms how they manage and secure their digital assets," said Ilyas Mohammed, COO at AmiViz. "The runZero Platform's ability to discover and unify data from IT, OT, IoT, cloud, mobile, and remote assets ensures that our clients can see and secure everything on their networks, leaving no blind spots."

Regional enterprises can now benefit from a holistic view of their security landscape, with the runZero Platform providing total visibility across diverse asset categories. On average, enterprises discover 25% more assets with runZero than they were previously aware of. This enhanced security posture is crucial in today's complex digital environment, where threats are continuously evolving, and the need for comprehensive management is paramount.

"We are excited to collaborate with AmiViz, a leader in the cybersecurity distribution space," said Joe Taborek, Chief Revenue Officer at runZero. "Our partnership ensures that Middle Eastern enterprises have access to cutting-edge technology that is essential for identifying and securing all assets on their networks, ultimately reducing their risk of cyber attacks."

QUALYS EXPANDS TRURISK ELIMINATE PLATFORM, EMPOWERING ORGANISATIONS TO MITIGATE CYBER RISK WITHOUT PATCHING

Qualys, Inc., a leading provider of disruptive cloud-based IT, security and compliance solutions, has unveiled TruRisk Eliminate, a comprehensive remediation solution that extends beyond patching to help organisations further reduce risk. It provides additional innovative remediation methods when patching isn't feasible. This approach uses patchless patching, targeted isolation, and other mitigation strategies to ensure robust protection.

Patch management is a core capability for remediating vulnerabilities, but it is not always the most viable or only option. Addressing all vulnerabilities is increasingly difficult due to potential business disruptions from patching, the unavailability of patches for zero days, and the limitations of traditional patch management tools that rely solely on agents. At-risk assets that can't be patched present vulnerabilities exploitable by hackers, leading to ransomware and data breaches. Cybersecurity and IT teams need effective mechanisms to mitigate the risks of unpatched vulnerabilities while maintaining business operations.

"Although patching is an essential part of vulnerability management to mitigate risk, there are some use cases where it isn't possible, or doing so requires outages or downtime that can impact operations. In some cases, such as new exploits or zero-day vulnerabilities, a patch may not even be available," said Melinda Marks, practice director, cybersecurity, at Enterprise Strategy Group. "Now with TruRisk Eliminate, Qualys augments its vulnerability management capabilities with an innovative solution to efficiently mitigate risk with patchless approaches to remediating vulnerabilities, helping security teams better align with and support business operations."

Qualys TruRisk Eliminate equips security and IT teams with powerful tools to enhance cybersecurity resilience by addressing critical vulnerabilities with or without deploying a patch. This solution reduces friction in current processes, enabling CISOs and CIOs to effectively reduce risk through patch management, configuration changes, mitigation, and targeted isolation. As a result, organisations can significantly lower their vulnerability exposure and streamline their response to cyber threats. TruRisk Eliminate provides more flexibility and options tailored to an organization's unique operational needs, remediation timelines, and business objectives.

SECUREWORKS DISCOVERS IDENTITY RISKS IN UNDER 90 SECONDS

Secureworks, a global leader in cybersecurity, has announced a new industry benchmark of 90 seconds to discover identity related risks and misconfigurations, an issue that impacts 95% of organisations. Launched today, Secureworks Taegis IDR, a new Identity Threat Detection and Response (ITDR) solution, proactively closes security gaps by leveraging advanced AI and machine learning, to automatically detect, prioritise and respond to identity-based threats across an organisation's environment and the dark web.

Identity remains one of the top three access vectors for ransomware and in the last three years, Secureworks Counter Threat Unit (CTU™) has observed a 688% increase in stolen credentials offered for sale on one of the dark web's largest marketplaces. Analysis of Microsoft Entra ID (formerly Microsoft Azure Active Directory) environments by the Secureworks Incident Response team has revealed that 95% are misconfigured, opening the door for cyber criminals to escalate privileges and carry out identity-based attacks. It's clear that the risk around identity is the unsolved puzzle of cyber, creating opportunities for threat actors to exploit and cause havoc.

"Identity is the fuel of the cybercriminal ecosystem and today we're cutting off their supply," stated Kyle Falkenhagen, Chief Product Officer, Secureworks. "Taegis IDR constantly monitors an organisation's environment and the dark web to automatically prevent, detect, prioritise and respond to identity-based threats that bypass traditional identity security controls. Unifying identity protection with the latest threat intelligence, AI, and broad visibility across endpoints, cloud and other applications, Taegis IDR uncovers misconfigurations to improve identity security posture with speed and precision."

WSO2 LAUNCHES MICRO INTEGRATOR 4.3, BRINGS AI ASSISTANCE TO INTEGRATION DEVELOPMENT

WSO2, a leading global provider of digital transformation technologies, unveiled the latest enhancements to WSO2 Micro Integrator. Version 4.3 of the advanced integration solution is set to redefine the developer experience by delivering enhanced capabilities and performance for modern application integration. With its latest updates, the solution offers a seamless integration of APIs, services, and systems, enabling organisations to better manage their integration workflows, reduce complexities, and accelerate time-to-market.

"For over a decade now, thousands of deployments have leveraged the power of WSO2 Micro Integrator to streamline connectivity among applications, services, data, and clouds. Now, as enterprises increasingly shift towards cloud-native architectures and microservices, the need for scalable and agile integration solutions has never been more crucial. With its expanded features and user-friendly interface, the new version empowers both seasoned developers and newcomers alike to create effective integration solutions that drive business growth and innovation," said Selvaratnam Uthaiyashankar, senior vice president & general manager - integration at WSO2.

Among its many new features, WSO2 Micro Integrator 4.3 introduces an enhanced integration flow designer. This provides an intuitive low code editor that simplifies the process of building integration flows. Developers can visually design integration sequences, eliminating the need for complex coding and enabling faster iteration cycles.

OPSWAT ACQUIRES INQUEST, STRENGTHENING GOVERNMENT GO-TO-MARKET STRATEGY, NETWORK DETECTION, AND THREAT INTELLIGENCE CAPABILITIES

OPSWAT, a global leader in critical infrastructure protection (CIP) cybersecurity solutions, has announced its acquisition of InQuest, a leading cybersecurity solutions provider known for its novel Deep File Inspection and RetroHunting technologies. InQuest is highly regarded for protecting the United States Department of Defense (DoD) customers with its network appliances that peer up to and beyond Layer 7, and combined with their threat intelligence solutions, have a proven track record of protecting the nation's most critical networks.

OPSWAT's relationship with InQuest has significantly grown since their technology partnership was established in 2013 when OPSWAT's MetaDefender module was integrated with InQuest's Network Detection and Respond solution for a joint customer at the United States Pentagon.

With this acquisition, OPSWAT will accelerate its go-to-market strategy for the government market and enhance protection against network-based threats. By merging InQuest's threat intelligence capabilities with OPSWAT MetaDefender Cloud and FileScan.io into a single repository, OPSWAT will significantly boost its intelligence capabilities. InQuest customers will also benefit from enhanced Network Detection and Response (NDR) with built-in integration with MetaDefender.

HUMAN VS AI

NED BALTAGI, MANAGING DIRECTOR, MIDDLE EAST, AFRICA, AND TURKEY, AT SANS INSTITUTE, TELLS ANITA JOSEPH THAT THE DEMAND FOR SKILLED PROFESSIONALS IN THE REGION CONTINUES TO OUTPACE SUPPLY EVEN AS AI-POWERED ATTACKS ARE BECOMING INCREASINGLY RAMPANT.

With the rise of AI-driven cyber threats, how has the cybersecurity skills gap evolved over the past few years, and what challenges does this pose for organisations in the Middle East?

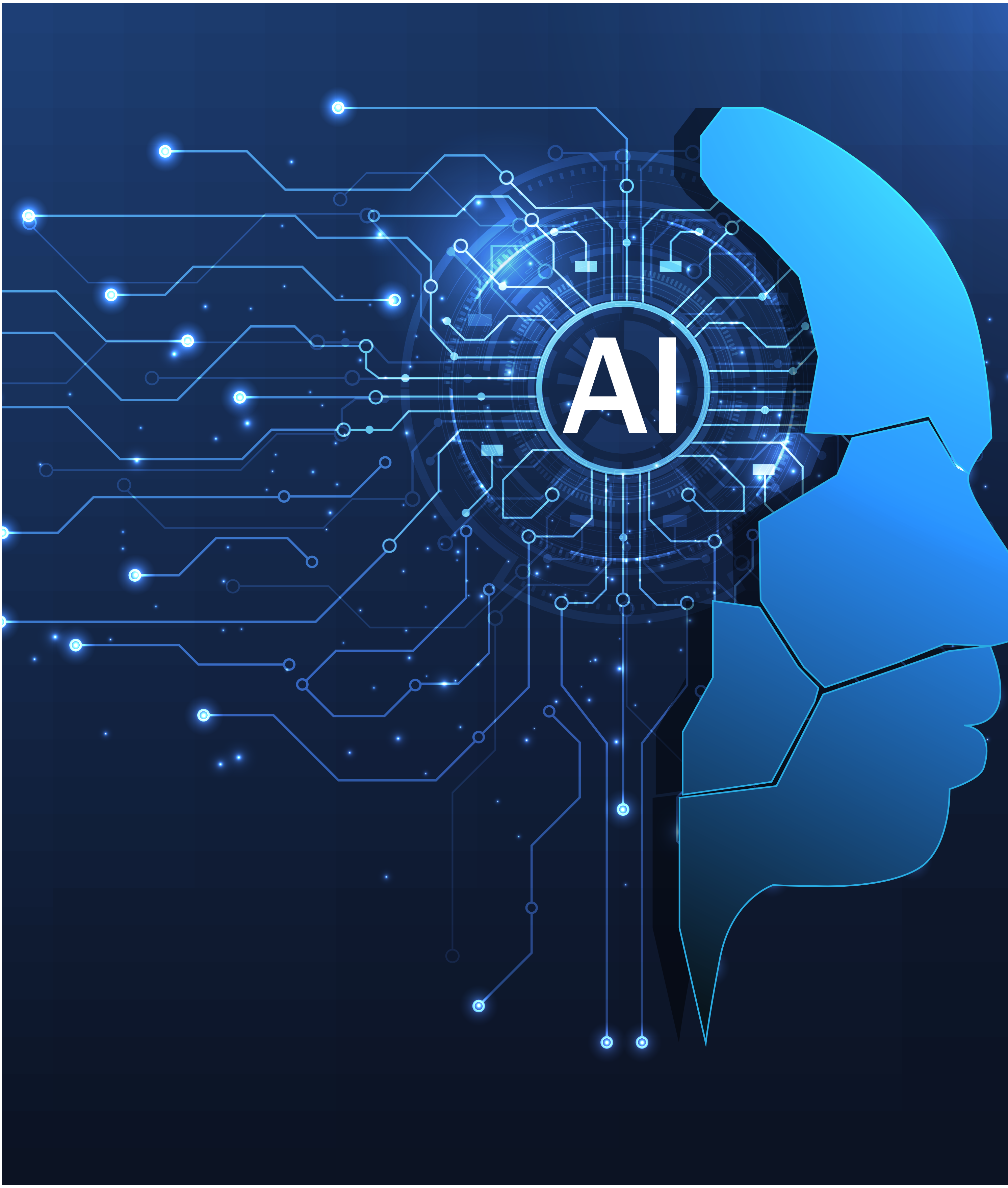
Over the past few years, the cybersecurity skills gap has widened significantly, particularly with the rise of AI-driven cyber threats. Globally, the cybersecurity workforce needs to grow by 3.4 million professionals to meet demand, and the Middle East is no exception, leaving organisations exposed to escalating risks.

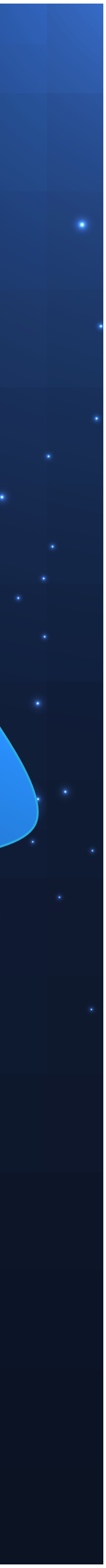
This shortage is particularly concerning as AI-powered attacks become more prevalent. Cybercriminals are now using AI to automate phishing campaigns, identify vulnerabilities, and launch sophisticated attacks. Meanwhile, many organisations in the Middle East are struggling to fill critical cybersecurity roles, leading to increased reliance on external consultants and AI-driven security solutions.

In the Middle East, there are still thousands of unfilled cybersecurity positions, despite a 7.1% decline in the workforce gap over the past year. Countries like the UAE and Saudi Arabia have experienced some improvements, but the demand for skilled professionals continues to outpace supply. The region's educational institutions are beginning to address this issue, but the pace is slow compared to the urgent need driven by technological advancements and the persistent threat landscape.

Consequently, organisations in the Middle East are increasingly turning to AI and automation to mitigate the impact of these talent shortages, but human expertise remains indispensable for tackling the most advanced cyber threats. The gap presents a dual challenge: finding qualified professionals and ensuring that they receive ongoing training to keep pace with the rapidly evolving threat landscape. The consequences of this shortage are clear—higher operational risks, increased costs, and the urgent need for strategic investments in cybersecurity education and AI-powered defences.

ORGANISATIONS IN THE MIDDLE EAST ARE INCREASINGLY TURNING TO AI AND AUTOMATION TO MITIGATE THE IMPACT OF TALENT SHORTAGES, BUT HUMAN EXPERTISE REMAINS INDISPENSABLE FOR TACKLING THE MOST ADVANCED CYBER THREATS.


AI



How does SANS Institute stay ahead of emerging technologies and threats in designing its courses to ensure cybersecurity professionals are equipped with the necessary skills?
At SANS, we are continuously reviewing and updating our programs and curriculum to incorporate new technologies, emerging threats, and recent incidents, so our students will always be one step ahead of the game. We have a team of world-renowned cybersecurity experts with real-world experience, whose research and insights directly inform course content. We also maintain ongoing collaborations with SANS government agencies, to ensure that local cyber talent is being discovered, nurtured and upskilled in different regions. Our courses include hands-on labs and simulations that reflect the latest attack techniques and defensive strategies, allowing students to gain practical experience that they can apply immediately once they are back at their jobs. We also offer advanced certifications for cybersecurity professionals long after completing their initial training, for those who wish to stay updated on new developments.

Moreover, at our training events, our teams and instructors engage with the global cybersecurity community through Community Nights, conferences, and forums. It's also important for us to gather regular feedback from this community, as well as from alumni, to help refine and expand our course offerings to address new challenges.

Could you elaborate on specific SANS courses that focus on AI-related threats and how they prepare students to tackle these challenges effectively?
We offer a wide range of training programs that demonstrate how AI and ML can be applied to enhance various cybersecurity roles. From courses to forums and webcasts, we showcase practical approaches to incorporating AI into daily tasks, making them more efficient and effective. We're also committed to advancing AI cybersecurity research through collaborations with academic and industry partners. Our goal is to ensure that AI is used responsibly and securely in cybersecurity solutions. Our research and guidance provide a solid foundation for organisations to implement effective AI security measures.

AIS247: AI Security Essentials for Business Leaders explores generative AI principles, applications, and associated risks with a focus on ethical usage and policy development. This course emphasizes enhancing productivity, ethically aligning cybersecurity teams, risk management, and responsible AI policies.

Coming soon, we will have SEC535: Offensive AI - Attack Tools and Techniques - which provides a foundational understanding of using AI for offensive purposes, covering security bypassing, exploit development, social engineering, automated attacks, and malware creation.

In your opinion, what are the key areas where traditional cybersecurity training might fall short in today's rapidly evolving landscape, and how does SANS address these gaps?
The pace of modernisation and adoption of emerging technologies, such as artificial intelligence (AI), cloud computing, and the Internet of Things (IoT), has significantly transformed the region's economic landscape. While these advancements offer immense opportunities, they also introduce new vulnerabilities that traditional cybersecurity methods may struggle to address. AI-powered attacks, sophisticated cloud-based threats, and the interconnected nature of IoT devices demand a more proactive and adaptive approach to cybersecurity. Traditional training methods, often focused on static threat models and outdated technologies, may not equip professionals with the skills needed to navigate these evolving challenges.

AT SANS, WE ARE CONTINUOUSLY REVIEWING AND UPDATING OUR PROGRAMS AND CURRICULUM TO INCORPORATE NEW TECHNOLOGIES, EMERGING THREATS, AND RECENT INCIDENTS.

We are committed to bridging this gap by offering immersive training experiences that equip cybersecurity professionals with the knowledge and skills necessary to protect against new threats – and we ensure our training is never monotonous and that students are constantly engaged. Our largest events in the Middle East, including the upcoming SANS Cyber Safari 2024 in Saudi Arabia and SANS Gulf Region 2024 in the UAE, feature a diverse range of practical courses designed to address the region's specific cybersecurity needs.

SANS Cyber Safari 2024 (October 5-24in Saudi Arabia offers 12 courses covering a wide range of topics, from foundational security principles to advanced threat hunting techniques, providing cyber professionals with the opportunity to enhance their security capabilities and stay ahead of the curve.

SANS Gulf Region 2024 (2-21 November in the UAE brings 15 courses, including in-depth training on Threat Hunting and Incident Response, Cloud Security, IoT Security, and Cybersecurity Leadership. These courses are designed with practical and immersive exercises, hands-on labs, and a variety of real-world simulations, to equip professionals with the practical skills and knowledge needed to protect critical infrastructure and data in the region.

TENABLE INTRODUCES AI AWARE FOR AI AND LARGE LANGUAGE MODELS

Tenable, the exposure management company, has announced the release of AI Aware, advanced detection capabilities designed to rapidly surface artificial intelligence solutions, vulnerabilities and weaknesses available in Tenable Vulnerability Management, the world's #1 vulnerability management solution. Tenable AI Aware provides exposure insight into AI applications, libraries and plugins so organisations can confidently expose and close AI risk, without inhibiting business operations.

The rapid development and adoption of AI technologies in the past two years has introduced major cybersecurity and compliance risks that organisations must proactively address without established best practices. As a result, cybersecurity teams face significant AI-related challenges, such as vulnerability detection and remediation, containing data leakage and reining in unauthorised AI use.

According to recent Tenable Research, more than one-third of security teams are finding usage of AI applications in their environment that might not have been provisioned via formal processes. In fact, during a 75-day period between late June and early September, Tenable found over 9 million instances of AI applications on more than 1 million hosts. The cybersecurity risk of unfettered AI usage is compounded by the increasing volume of AI vulnerabilities. Tenable Research has found and disclosed several vulnerabilities in AI solutions, including in Microsoft Copilot, Flowise, Langflow, among others.

With AI Aware, Tenable transforms proactive security for AI solutions. Tenable AI Aware uniquely leverages agents, passive network monitoring, dynamic application security testing and distributed scan engines to detect approved and unapproved AI software, libraries and browser plugins, along with associated vulnerabilities, thereby mitigating risks of exploitation, data leakage and unauthorized resource consumption. The combined depth of these multiple assessment methods delivers the most complete detection of AI in the modern ecosystem.

In addition to AI software and vulnerability detection, key AI Aware features available in Tenable Vulnerability Management, Tenable Security Center and Tenable One include:

- Dashboard Views provide a snapshot of the most common AI software discovered in the ecosystem, top assets with vulnerabilities related to AI and the most common communication ports leveraged by AI technologies.
- Shadow Software Development Detection illuminates the unexpected existence of the building blocks of AI development in the environment, enabling businesses to align initiatives with organizational best practices.
- Filter Findings for AI Detections enable teams to focus on AI-related findings when reviewing vulnerability assessment results. Combined with the power of Tenable Vulnerability Prioritization Rating (VPR), teams can effectively assess and prioritize vulnerabilities introduced by AI packages and libraries.
- Asset-Centric AI-Inventory provides a complete inventory of AI-related packages, libraries and browser plugins while reviewing the detailed profile of an asset.

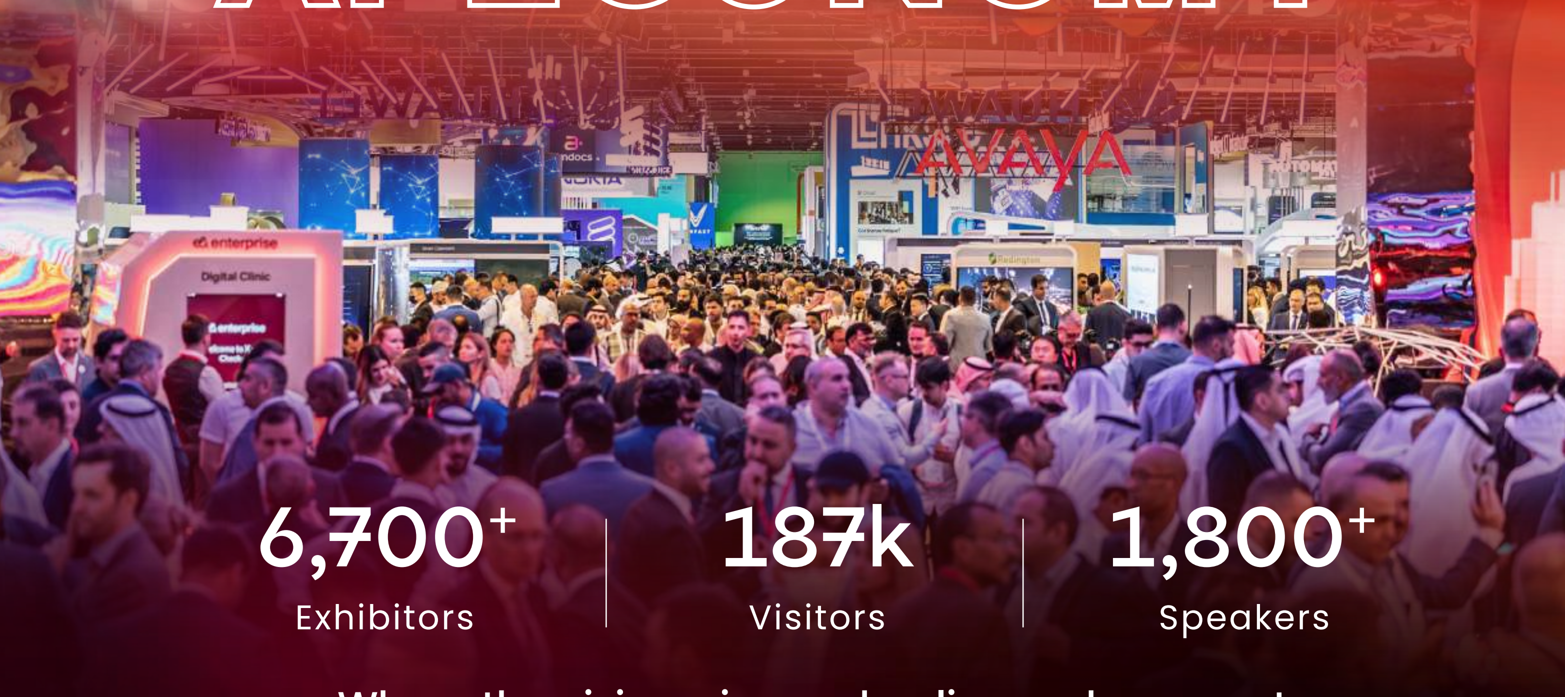
GITEX GLOBAL

14 - 18 OCT 2024
DUBAI WORLD TRADE CENTRE

MON	TUE - FRI
11 AM - 5 PM	10 AM - 5 PM

THE LARGEST TECH & STARTUP
EVENT IN THE WORLD

Global Collaboration to Forge a Future AI ECONOMY



6,700+	187k	1,800+
Exhibitors	Visitors	Speakers

Where the visionaries and policy makers meet.

#GITEXGLOBAL
gitex.com

Scan the QR code to
SECURE YOUR PASS

ORGANISED BY
مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

INDUSTRY LEADERS LAUNCH 3M DATA IN SAUDI ARABIA: A NEW CHAPTER IN INNOVATION AND MARKET LEADERSHIP

In a move poised to redefine the tech and data industries in the Middle East, three seasoned technology industry leaders—Mohamad Hejazi, Mohamad Jamous, and Musa Kazim—have come together to launch 3M Data in Saudi Arabia. This strategic collaboration marks a significant technological milestone, combining decades of experience to drive innovation and deliver advanced, tailored solutions across various key sectors.

3M Data builds the technological foundation for the Middle East's most exciting projects. It synergizes Next-Gen Cloud Architecture, Digital Infrastructure, Cybersecurity and Managed Services to create and deploy digital transformation of the highest standards, for cutting-edge projects that improve the way we live and work.

Mohamad Hejazi, General Manager of 3M Data, highlighted the foundation of the new company and the vision that drives this venture. He stated, "The journey of 3M Data began with three industry leaders who have been in the market for over 15 years, particularly in the Saudi Arabian and Middle Eastern markets. We worked closely together in our previous roles, achieving significant success and delivering exciting projects. After years of collaborating and understanding the market's needs, we decided to come together and take on a new challenge. Our goal was to create a company that could exceed client expectations and provide even more comprehensive solutions than we had in the past." Building on this foundation, 3M Data aims to harness the collective experience of its leadership team to elevate the company to new heights in the region.

"The Saudi market is a dynamic landscape full of opportunities, and we are eager to be part of its ongoing transformation and growth," said Mohamad Jamous, Sales Director at 3M Data. "We look forward to contributing to its Vision 2030 goals and playing a role in shaping the future narrative of the country's remarkable journey."

Musa Kazim, Services Director, emphasized that 3M Data will help organizations navigate their digital transformation journey seamlessly, ensuring they maximize the benefits of their technology investments. "As a leader in innovation, 3M Data is poised to make significant contributions to key industries. By leveraging cutting-edge technology and science-based performance, we are committed to delivering extraordinary outcomes for our clients and driving economic growth in the region," he said.

The launch of 3M Data in Saudi Arabia represents more than just the entry of a company into a new market. It symbolizes the fusion of expertise with experience, addressing the unique challenges and opportunities within the Middle East. With a proven track record and a forward-thinking approach, 3M Data is set to become a pivotal player in the region's digital transformation journey.

3M DATA AIMS TO HARNESS THE COLLECTIVE EXPERIENCE OF ITS LEADERSHIP TEAM TO ELEVATE THE COMPANY TO NEW HEIGHTS IN THE REGION.

SECURING THE FUTURE

MANDAR PATIL, SVP-META SAARC & ASEAN AT CYBLE TELLS ANITA JOSEPH HOW AN INTELLIGENT APPROACH TO THREAT DETECTION IS HELPING THE COMPANY SECURE THE DIGITAL FUTURE OF BUSINESSES IN THE REGION.

Tell us about Cyble and its activities in the region.

Cyble, established in 2019 with its headquarters in Atlanta, USA, is a leading threat intelligence company. We are among the few service providers globally to offer an integrated, AI-enabled next-generation platform that combines digital risk protection, incident response, attack surface monitoring, threat intelligence, and third-party risk monitoring. With a focus on gathering intelligence from the deep, dark, and surface web, Cyble has quickly positioned itself as a pioneer in the industry. Our innovative work has been recognised by esteemed organisations such as Gartner, Forrester, Frost & Sullivan, and even Forbes.

Building on strong business growth, Cyble has expanded its presence to 22 countries, serving over 500 clients, globally. Our story in the Middle East is an exciting one. Middle East has been our fastest-growing region, with a robust presence in the UAE and Saudi Arabia, we have a network of over 53 partners in the region, including some of the largest managed security service providers (MSSPs). Cyble's customers span diverse industries, including IT, Telecom, Retail, Banking, Insurance, and Government. Our contributions to the cybersecurity community have been widely recognised by major organisations such as Facebook, Cisco, and the U.S. Government.

What makes Cyble a strong choice amid industry acquisitions?

In 2024, as several threat intelligence companies are acquired by larger corporations, businesses are experiencing shifts in how their security

needs are addressed. These acquisitions often result in reduced innovation, corporate-driven priorities, and less flexibility.

Cyble stands out by remaining independent, fully focused on cybersecurity. This independence allows Cyble to prioritise customer-centric innovations, free from the constraints of corporate integration, delivering tailored solutions for each organisation's unique needs.

Cyble's commitment to data privacy is another key differentiator. Customers retain full control of their data, ensuring transparency and security. In contrast to many competitors now integrated into financial ecosystems, Cyble's customizable solutions enable organisations to address their specific security challenges without being locked into rigid frameworks. This flexibility ensures that Cyble's solutions can evolve alongside businesses, making it the ideal choice in today's rapidly shifting market.

WE HAVE A CYBLE TEAM BASED IN THE REGION, WITH OFFICES SERVING OVER 100 CUSTOMERS AND MORE THAN 53 PARTNERS.

How is Cyble leveraging AI to offer comprehensive cyber protection to its clients?

At Cyble, we were early adopters of artificial intelligence, integrating AI into our platform well before the advent of Generative AI. While many companies are just beginning to explore Generative AI,

Cyble had already incorporated AI into key services by 2021.

Cyble's enterprise threat intelligence platform, Vision, harnesses a combination of custom AI models and Generative AI-based large language models (LLMs). This combination is used in automated analysis, threat context extraction, translation, summarisation, and risk prioritisation, all of which are applied to petabytes of data and billions of records processed daily. This advanced AI utilisation provides our clients with unmatched visibility into the global and regional threat landscape, dramatically enhancing their situational awareness and enabling them to take proactive action before a threat becomes an incident.

AT CYBLE, WE WERE EARLY ADOPTERS OF ARTIFICIAL INTELLIGENCE, INTEGRATING AI INTO OUR PLATFORM WELL BEFORE THE ADVENT OF GENERATIVE AI.

In addition to Vision, Cyble Hawk is our advanced platform, specifically designed for federal bodies, governments, and defence sectors, offering an even more comprehensive and focused approach to intelligence and threat detection. By combining OSINT with enhanced investigative techniques, Cyble Hawk delivers deep, actionable intelligence beyond surface-level data. Utilising AI and deep learning, it tracks threats and identifies known threat actors, keeping organisations ahead of evolving risks. With real-time monitoring, it provides precise advisories on vulnerabilities, compromised credentials, and breaches

CYBLE OFFERS PEACE OF MIND, SECURING YOUR FUTURE WITH ROBUST CYBERSECURITY.

impacting critical sectors. Additionally, Cyble Hawk delivers timely intelligence on extremist actions, cybercrime, and financial crime, such as blockchain-based money laundering, ensuring constant protection and situational awareness.

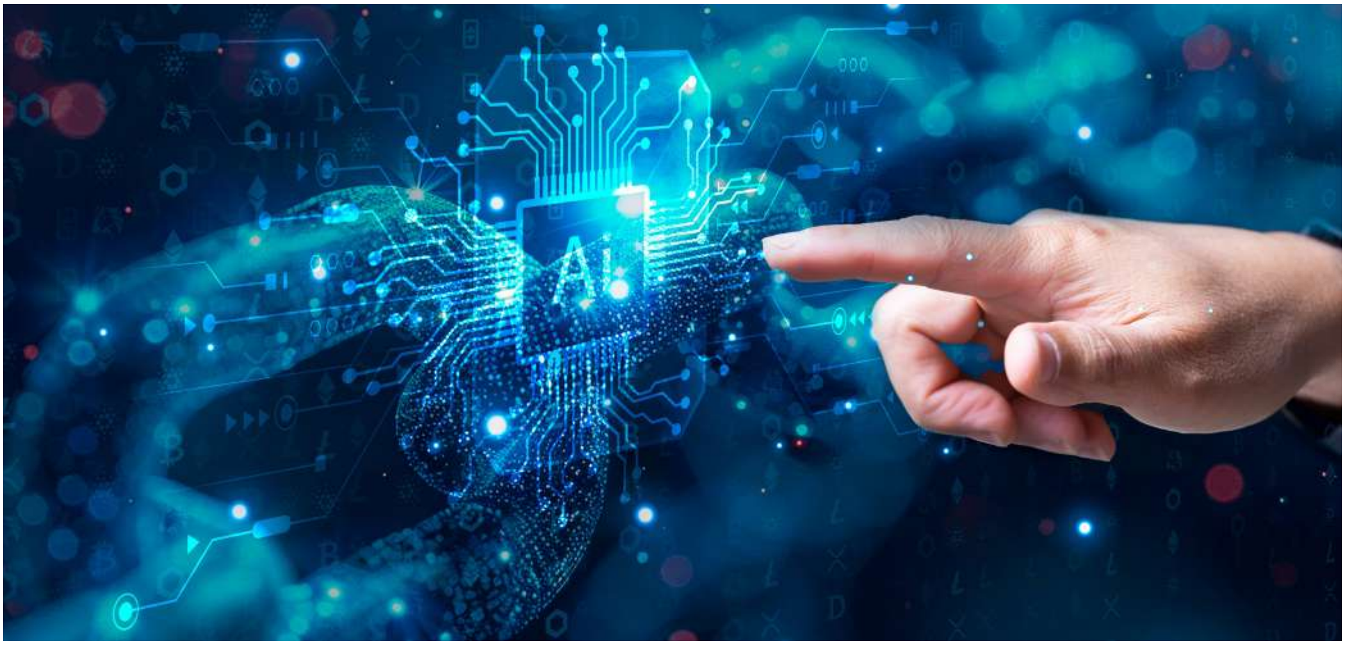
What sets Cyble apart in terms of proactive cybersecurity?

Cyble offers peace of mind, securing your future with robust cybersecurity. Our primary goal is to provide clients with early warning intelligence that helps prevent or neutralise cyberattacks before they manifest. Our platform delivers a comprehensive suite of proactive cybersecurity capabilities, enabling defenders and analysts to detect and mitigate threats at the earliest stage.

For instance, our Threat Intelligence Module enables clients to monitor conversations on the dark web and cybercrime forums for any signs of compromised user identities, applications, or systems. It also helps discover exposed confidential data belonging to the organisation or its users. Cyble maintains an extensive repository of over 1 billion indicators of compromise (IoCs), which customers use for automatic enrichment, correlation, and blocking of security events.

Our Vulnerability Intelligence Module, powered by a global network of honeypots and supported by our vulnerability researchers, tracks zero-day vulnerabilities and actively exploited weaknesses. It also monitors malicious exploits being traded on dark web marketplaces, allowing clients to prioritize patching critical security issues. This approach enables risk-based prioritisation in patch management.

Additionally, our Brand and Social Monitoring service, along with our Incident Response Service, identifies and takes down suspicious and phishing domains before they are used in stealth attacks. Many large enterprises rely on Cyble for executive protection services to safeguard sensitive personal information. Cyble offers some of the industry's best takedown service level agreements (SLAs) globally.



Cyble's Third-Party Risk Monitoring Capabilities are widely used by our clients to assess the cybersecurity posture of their vendors, categorise them based on security exposure, and implement focused remediation strategies as part of their supplier risk management processes. This helps proactively reduce third-party risk to their business.

In addition to our advanced platform capabilities, Cyble's competitive edge lies in the quality and expertise of our global threat research team. This highly skilled team specialises in human intelligence (HUMINT), open-source intelligence (OSINT), tradecraft, malware analysis, reverse engineering, incident response, and forensics.

With proficiency in languages such as Russian, Romanian, Arabic, and Chinese, our researchers gather intelligence from dark web and cybercrime forums, often preventing or helping investigate high-profile incidents for our clients.

Our threat research team consistently hunts, analyses, and reports on emerging threat campaigns, rapidly evolving techniques, and the tools used by threat actors. The team has played a critical role in responding to and investigating several high-profile incidents, particularly in the APAC and Middle Eastern regions.

Cyble's Managed Threat Intelligence Services help nearly 500+ clients globally operationalize threat intelligence within their organisations through a consultative and collaborative approach.

A key differentiator for Cyble is our multi-tenant, MSSP-ready platform. This platform allows MSSP partners to easily onboard their customers within hours and offer managed threat intelligence services, including monitoring, analysis, and reporting, through a single, secure console. The Vision platform caters to the threat intelligence needs of security researchers, threat intelligence analysts, and decision-makers, delivering a feature-rich stack of services through one platform. For instance, MSSPs can generate and publish custom or targeted intelligence and alerts via the platform, significantly amplifying the value of the threat intelligence for their end customers.

OUR PRIMARY GOAL IS TO PROVIDE CLIENTS WITH EARLY WARNING INTELLIGENCE THAT HELPS PREVENT OR NEUTRALISE CYBERATTACKS BEFORE THEY MANIFEST.

What are Cyble's future plans for the region?

Given the overwhelmingly positive feedback from our customers and partners, Cyble anticipates a significant increase in demand for our services in the Middle East. We continue to invest heavily in the region and are expanding our field staff to meet the growing business demand from customers and heightened interest from MSSP partners and resellers.

Currently, we have a Cyble team based in the region, with offices serving over 100 customers and more than 53 partners, supported by Cyble-certified solution engineers. In response to growing customer demand, Cyble is slated to introduce several exciting new features and services, focusing on Deepfake detection, cloud security, physical security, and advanced digital forensics and incident response capabilities in the Middle East.

SKILLS GAP LEAVES ORGANISATIONS OPEN TO NEW THREATS

ROB RASHOTTE, VICE PRESIDENT, GLOBAL TRAINING & TECHNICAL FIELD ENABLEMENT AT FORTINET

With nearly 4 million professionals needed to fill critical cybersecurity roles, organisations around the globe are feeling the impact of the ongoing skills gap. Breaches can rarely be attributed to a single cause, yet 58% of leaders indicate that a lack of IT and cybersecurity skills and training within their organisation contributes to security incidents.

All it takes is a single cyber incident to open any organisation to new threats and vulnerabilities. For example, following a breach, threat actors now have valuable insights about an enterprise's environment that they can use to craft a new attack. Others may attempt to capitalise off a previous breach, viewing a recently compromised organisation as low-hanging fruit. While understanding and taking steps to mitigate these risks is crucial, what is often even more concerning, especially to those in C-level positions and on the board of directors, is the potential impact these incidents can have on business operations.

That's why closing risk management strategy gaps, including addressing critical resources like staffing, is vital to protect any organisation effectively.

The Skills Shortage Increases Cyber Risks, Leading to New Threats and Vulnerabilities

Cybercriminals continue to advance their operations, refining well-known attack methods and using generative AI to speed their efforts. Therefore, it's not surprising that cybersecurity incidents are rising worldwide. According to Fortinet's 2024 Cybersecurity Skills Gap Report, almost 90% of businesses experienced one or more security breaches last year, up from 84% in 2024 and 80% in 2021. The dire need for skilled cybersecurity professionals puts businesses at a disadvantage: Nearly three-quarters of leaders agree that the cybersecurity skills gap creates additional risks for their enterprise.

Breaches are equally common across all regions, with the average number of breaches per organization in Asia Pacific being the highest (3.18) and Latin America being the lowest (2.79). And the percentage of organisations that report suffering no breaches at all continues to shrink—just 13% of businesses had zero breaches in 2023 compared to 15% the year before and 20% in 2021.

As Breaches Rise, the Threat Landscape Remains Familiar

While organizations increasingly fall victim to cybercriminals, the attacks used to compromise networks are familiar to defenders.

Malware, phishing, and web attacks combined accounted for 80% of all attacks organisations experienced yearly. Password attacks were more common in North America, and leaders in APAC experienced a higher percentage of phishing and web attacks than in other regions.

Cyber Incidents Have Far-Reaching Impacts

Cybersecurity incidents have increasingly significant impacts on organisations, ranging from financial to reputational challenges. More than half (53%) of leaders say breaches cost their organizations over $1 million in 2023, with North America and APAC reporting the most financially damaging attacks. Regarding recovery time, 63% said it took more than one month to bounce back from a cyberattack, with the average time being nearly three months.

In addition to monetary ramifications and lengthy recovery times, corporate leaders are held accountable when breaches occur: 51% of IT and security leaders say that board members or executives have faced fines, jail time, loss of their position, and loss of employment following a cyberattack.

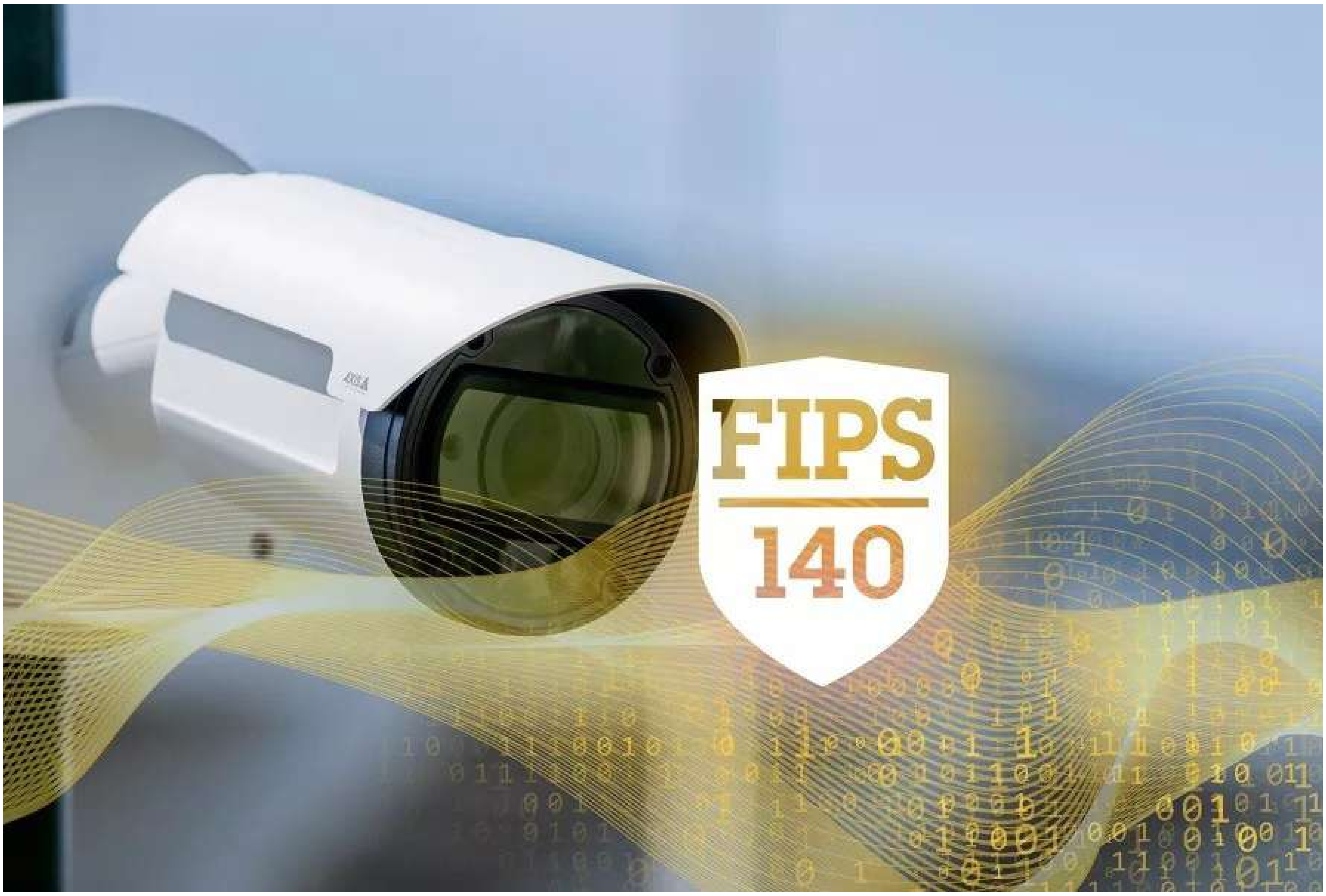
A Robust Cybersecurity Program Requires Technology, Training, and Awareness

The stakes are high for organisations when it comes to cybersecurity. Breaches continue to take a financial toll, and senior leaders are sometimes penalised when they happen. With the growing skills gap creating additional risks for organisations, many businesses are embracing new, creative approaches to recruiting, hiring, and retaining skilled professionals. It's encouraging that leaders pursue unique initiatives and collaborate across the public and private sectors to address this challenge, as this is a crucial piece of the puzzle when it comes to strengthening an organization's overall defences.

Given these complexities, organisations should focus on a three-pronged approach to cybersecurity that blends technology, training, and awareness. Fortinet offers the most extensive integrated portfolio of over 50 enterprise-grade products through our Fortinet Security Fabric platform. Additionally, the award-winning Fortinet Training Institute, one of the industry's broadest training and certification programs, is dedicated to making cybersecurity certification and new career opportunities available to everyone and offering current professionals the chance to advance their skill sets. The institute offers a variety of free and low-cost education and certification programs, unique initiatives to upskill and reskill individuals from diverse backgrounds, and more. The Fortinet Training Institute also has a Security Awareness Training offering designed to help organizations cultivate a more cyber-aware workforce.

Cybercriminals aren't slowing down anytime soon, making cybersecurity an "all hands on deck" effort for every organisation. Highly skilled professionals with access to the right cybersecurity technologies are essential to protecting businesses from breaches, as is having cyber-aware employees who can serve as a solid first line of defence. By refreshing and strengthening distinct aspects of a risk management strategy, an enterprise will be better positioned to defend against the speed and volume of today's attacks.

CLOSING RISK MANAGEMENT STRATEGY GAPS, INCLUDING ADDRESSING CRITICAL RESOURCES LIKE STAFFING, IS VITAL TO PROTECT ANY ORGANISATION EFFECTIVELY.



AXIS LAUNCHES FIRST FIPS 140-3-COMPLIANT DEVICE

Axis Communications, a leader in network video, is the first to launch a network security device with an embedded discrete secure element validated to the state-of-the-art FIPS 140-3 Standard Level 3. Thus, Axis customers in government and critical infrastructure can be assured that their devices live up to the security levels defined by the US National Institute of Standards and Technology (NIST) and required by law. FIPS 140-3 certification assesses four levels of security. At Level 3, hardware is expected to prevent tampering, and access must be identity based. The embedded discrete secure element, EdgeLock SE052F, is from NXP Semiconductors, a world leader in secure connectivity solutions for embedded applications and known for its trusted security solutions, including securing today's smartphones, bank cards and passports.

More devices with FIPS 140-3-validated secure elements on the way

Going forward, Axis will continue to expand its range of FIPS 140-3 certified devices by embedding the new secure element in all its upcoming network products. FIPS 140-3-compliance will be available for use cases ranging from surveillance to business optimisation (through analytics), to access control, and audio. Even organisations that are not required to comply with the high FIPS standards will benefit as they can also be confident that their systems are interoperable and will meet long-term security requirements.

Protection from the inside out

Ongoing investment in a portfolio equipped with industry-standard cryptographic computing modules is part of a multi-layer Axis strategy. Secure storage and computing of cryptographic keys is just one component of the hardware-based cybersecurity platform Axis Edge Vault. Axis Edge Vault also includes features like secure boot, and the IEEE 802.1AR-compliant Axis device ID that verifies the identity and authenticity of Axis devices.

SMART MEETS SUSTAINABLE

ARAFAT YOUSEF, MANAGING DIRECTOR, MIDDLE EAST & AFRICA AT AGINODE, TELLS ANITA JOSEPH HOW THE COMPANY COMBINES TECHNICAL EXPERTISE AND A FOCUS ON SUSTAINABILITY, TO OFFER WORLD-CLASS NETWORK MANAGEMENT SOLUTIONS FOR CUSTOMERS.

WE COLLABORATE WITH LOCAL PARTNERS AND DISTRIBUTORS TO FACILITATE SWIFT AND EFFECTIVE SERVICE WHILE SUPPORTING SUSTAINABILITY GOALS WITH ENERGY-EFFICIENT SOLUTIONS.

Tell us how Aginode's solutions align with the goals of the region's vision for digital and technology transformation, particularly in terms of supporting enterprise growth.
Aginode's solutions provide insights into local market needs and regulatory requirements, ensuring they are well-suited for the region. We adapt approaches that uniquely fit the cultural and business practices of the Middle East. We also offer expert technical support for training, design, configuration, and troubleshooting. Additionally, Aginode delivers customised solutions that address specific regional challenges and requirements.

Furthermore, we ensure that our solutions meet the high power and heat management needs commonly found in the Middle Eastern climate. We collaborate with local partners and distributors to facilitate swift and effective service while supporting sustainability goals with energy-efficient solutions. Lastly, we actively seek and incorporate customer feedback to improve our solutions and services while providing continuous support and updates to ensure our solutions remain effective and relevant.

Can you provide more details about your flagship enterprise networking and data centre solutions, specifically the Category 6A/7A high-end structured cabling? How do these solutions support high bandwidth needs and smart building technologies?
Aginode provides the market with smart solutions offering the best bandwidth by using Category 6A (Cat 6A) with a frequency of up to 500 MHz and a data rate of 10 Gbps over 100 meters with individual or overall shielding. It is applied in high-speed ethernet networks and enterprise environments and has reduced crosstalk while being future-proof for 10G Ethernet.

It supports up to 10 Gbps, which is sufficient for demanding applications like high-definition video streaming and large data transfers. It also has enhanced shielding that reduces crosstalk and external noise, ensuring stable and reliable connections for high-bandwidth applications. Lastly, it supports emerging technologies and high-speed network requirements, which is crucial as smart building systems evolve.

Category 7A (Cat 7A) on the other hand has a frequency of up to 1000 MHz and a data rate of 10 Gbps over 100 meters. It comes with superior shielding foil for each pair and overall. It can be applied in high-performance networks and data centers as it has superior shielding, supports higher frequencies and has minimal interference.

This solution supports up to 10 Gbps with a frequency of 1000 MHz, handling even higher data rates and more intense network traffic. It also features superior shielding with individual and overall foil which minimizes interference and ensures data integrity. Additionally, this provides robust and reliable connectivity for smart building technologies such as IoT devices, smart lighting, HVAC systems, and security systems, thereby ensuring seamless operation and high performance for all connected devices.

Both the cabling types contribute to the efficiency and effectiveness of smart buildings by enabling high-speed, reliable data transmission essential for complex and interconnected systems.

LANsense is touted as a comprehensive Automated Infrastructure Management system. Could you discuss how LANsense optimises network management, and what unique advantages it offers in terms of identifying disconnections and streamlining overall network management?
Aginode LANsense optimises network management with its key features including Automated Discovery, which offers real-time mapping of network devices and connections, Centralised Dashboard with unified interface for easy management and monitoring, and Detailed Reporting which provides insights into performance, capacity, and usage. It also helps maintain accurate, efficient, and scalable network management.

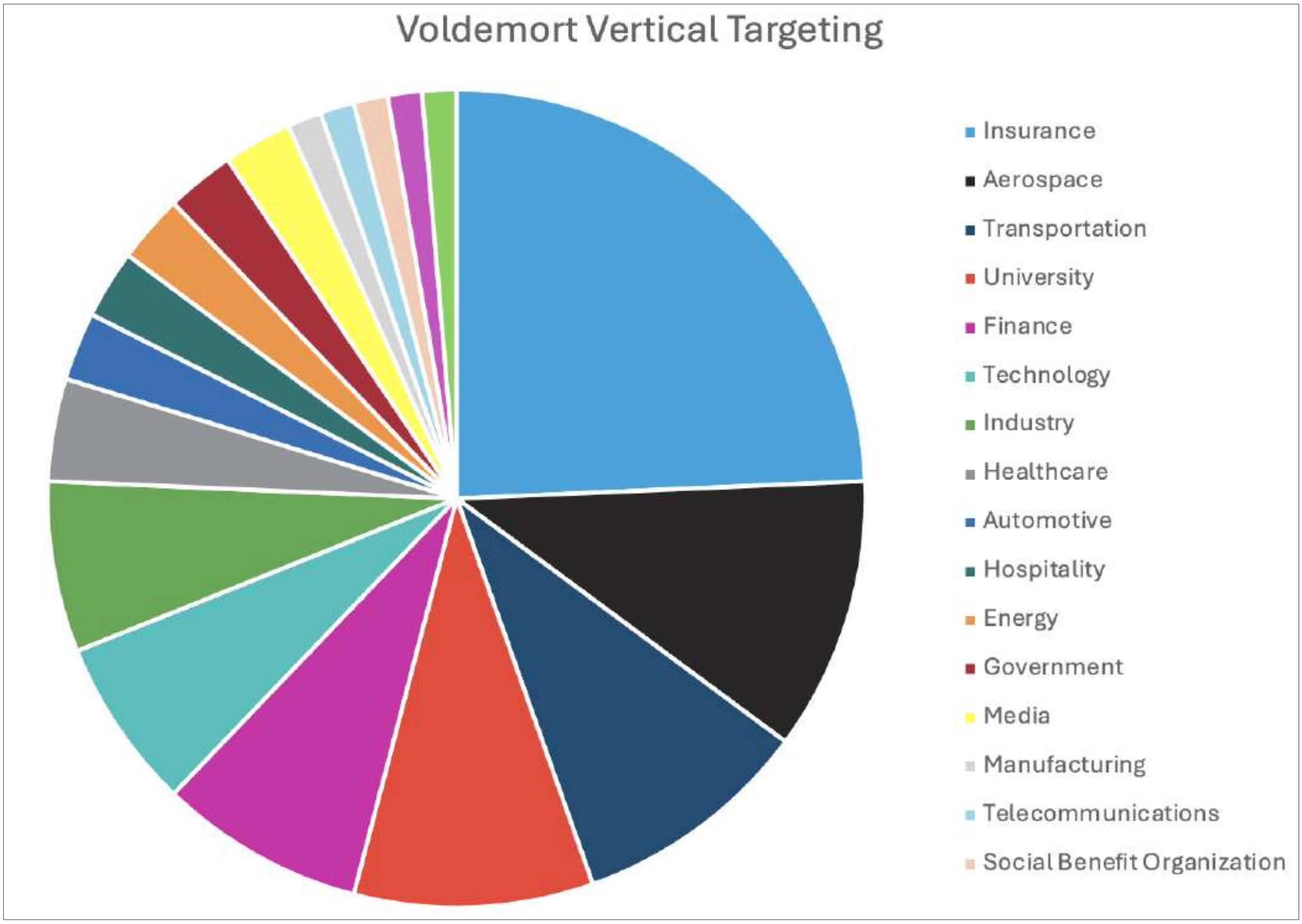
Some of its advantages include efficient disconnection identification, offering real-time alerts and diagnostics for quick issue resolution. It also provides streamlined management through automated updates and simplified troubleshooting. Enhanced visibility is achieved through comprehensive views and historical data for better planning, while seamless integration with other IT management systems is another key benefit. Additionally, the system offers scalability, adapting to the growing needs of the network.

In light of global emphasis on sustainability, how do Aginode's solutions, particularly those supporting POE with high power levels and excellent heat dissipation, contribute to energy-efficient performance and environmental responsibility?
Our LANactive solution supports PoE with high power levels and excellent heat dissipation, thereby contributing to energy efficiency and environmental responsibility. By supporting higher power levels such as PoE+ and UPOE, we enable more devices to be powered through a single cable. This reduces the need for additional power supplies and wiring.

Advanced PoE technology ensures power is used efficiently, minimising waste and optimising energy consumption for connected devices. Also, its excellent heat dissipation mechanisms prevent overheating, which helps maintain optimal performance and extends the lifespan of the equipment. Consequently, this reduces the need for additional cooling systems, lowering overall energy consumption. Additionally, proper heat management minimises the risk of equipment failure, reducing maintenance needs and the associated energy and resource usage.

Furthermore, PoE minimises the cables required for powering devices, reducing material use and waste. Our solutions have a lower carbon footprint as we improve energy efficiency and reduce the need for extra power infrastructure. Lastly, it integrates with smart building systems to optimise energy usage and reduce waste, contributing to greener building operations.

THE MALWARE THAT MUST NOT BE NAMED: SUSPECTED ESPIONAGE CAMPAIGN DELIVERS "VOLDEMORT"



In August 2024, Proofpoint researchers identified an unusual campaign using a novel attack chain to deliver custom malware. The threat actor named the malware "Voldemort" based on internal filenames and strings used in the malware.

The attack chain comprises multiple techniques currently popular within the threat landscape as well as uncommon methods for command and control (C2), like the use of Google Sheets. Its combination of tactics, techniques, and procedures (TTPs), lure themes impersonating government agencies of various countries, and odd file naming and passwords like "test" are notable.

Researchers initially suspected the activity may be a red team. However, the large volume of messages and analysis of the malware very quickly indicated it was a threat actor.

Proofpoint assesses with moderate confidence this is likely an advanced persistent threat (APT) actor with the objective of intelligence gathering.

However, Proofpoint does not have enough data to attribute with high confidence to a specific named threat actor (TA). Despite the widespread targeting and characteristics more typically aligned with cybercriminal activity, the nature of the activity and capabilities of the malware show more interest in espionage rather than financial gain at this time.

Voldemort is a custom backdoor written in C. It has capabilities for information gathering and to drop additional payloads. Proofpoint observed Cobalt Strike hosted on the actor's infrastructure, and it is likely that is one of the payloads that would be delivered.

Beginning on 5 August 2024, the malicious activity included over 20,000 messages impacting over 70 organizations globally. The first wave of messages included a few hundred daily but then spiked on 17 August with nearly 6,000 total messages.

Messages purported to be from various tax authorities notifying recipients about changes to their tax filings. Throughout the campaign, the actor impersonated tax agencies in the U.S. (Internal Revenue Service), the UK (HM Revenue & Customs), France (Direction Générale des Finances Publiques), Germany (Bundeszentralamt für Steuern), Italy (Agenzia delle Entrate), and from August 19, also India (Income Tax Department), and Japan (National Tax Agency). Each lure was customized and written in the language of the authority being impersonated.

Proofpoint analysts correlated the language of the email with public information available on a select number of targets, finding that the threat actor targeted the intended victims with their country of residence rather than the country that the targeted organisation operates in or country or language that could be extracted from the email address. For example, certain targets in a multi-national European organisation received emails impersonating the IRS because their publicly available information linked them to the US. In some cases, it appears that the threat actor mixed up the country of residence for some victims when the target had the same (but uncommon) name as a more well-known person with a more public presence. Emails were sent from suspected compromised domains, with the actor including the agency's real domain in the email address.

ITS COMBINATION OF TACTICS, TECHNIQUES, AND PROCEDURES, LURE THEMES IMPERSONATING GOVERNMENT AGENCIES OF VARIOUS COUNTRIES AND ODD FILE NAMING AND PASSWORDS ARE NOTABLE.

The threat actor targeted 18 different verticals, but nearly a quarter of the organizations targeted were insurance companies. Aerospace, transportation, and university entities made up the rest of the top 50% of organisations targeted by the threat actor.

Proofpoint does not attribute this activity to a tracked threat actor. Based on the functionality of the malware and collected data observed when examining the Sheet, information gathering was one objective of this campaign. While many of the campaign characteristics align with cybercriminal threat activity, we assess this is likely espionage activity conducted to support as yet unknown final objectives.

The Frankensteinian amalgamation of clever and sophisticated capabilities, paired with very basic techniques and functionality, makes it difficult to assess the level of the threat actor's capability and determine with high confidence the ultimate goals of the campaign. It is possible that large numbers of emails could be used to obscure a smaller set of actual targets, but it's equally possible the actors wanted to genuinely infect dozens of organisations. It is also possible that multiple threat actors with varying levels of experience in developing tooling and initial access worked on this activity. Overall, it stands out as an unusual campaign.

The behavior combines a variety of recently popular techniques observed in several disparate campaigns from multiple cybercriminal threat actors that have used similar techniques as part of ongoing experimentation across the initial access ecosystem. Many of the techniques used in the campaign are observed more frequently in the cybercriminal landscape, demonstrating that actors engaging in suspected espionage activity often use the same TTPs as financially motivated threat actors.

While the activity appears to align with espionage activity, it is possible that future activities associated with this threat cluster may change this assessment. In that case, it would indicate cybercriminal actors, while demonstrating some typical e-crime delivery characteristics, used customised malware with unusual features currently only available to the operators and not abused in widespread campaigns, as well as very specific targeting not normally seen in financially motivated campaigns.

Defense against observed behaviors includes restricting access to external file sharing services to only known, safelisted servers; blocking network connections to TryCloudflare if it is not required for business purposes; and monitoring and alerting on use of search-ms in scripts and suspicious follow-on activity such as LNK and PowerShell execution.

Proofpoint reached out to our industry colleagues about the activities in this report abusing their services, and their collaboration is appreciated.

DUBAI ELECTRONIC SECURITY CENTER LAUNCHES DUBAI AI SECURITY POLICY

Dubai Electronic Security Center (DESC) has announced the launch of the Dubai AI Security Policy, marking a proactive and pioneering step in the region. This policy aims to bolster confidence in AI solutions and technologies, promote their growth and development, and mitigate electronic security risks.

The unveiling of the new policy took place during the Dubai Cyber Security Center's participation as the official cybersecurity partner in the inaugural Dubai AI & Web3 Festival 2024. The event, organized by the Dubai AI Campus in cooperation with the Artificial Intelligence, Digital Economy and Remote Work Applications Office, and the Dubai International Financial Centre, was held in Madinat Jumeirah from 11-12 September.

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER
Number of A
Worldwide fr
2024
2030
Users in millions
Statista
DUBAI
AI & WEB3 FESTIVAL
Enabling Digital Economies

Harnessing Artificial Intelligence

His Excellency Yousuf Al Shaibani, CEO of the Dubai Electronic Security Center: "The launch of the AI Security Policy underscores Dubai Cyber Security Center's commitment to achieving the vision of the UAE's wise leadership, and the directives of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President, Prime Minister and Ruler of Dubai. This vision aims to position the UAE a global leader in AI by 2031, with the goal of developing an integrated system that harnesses AI in key sectors under the UAE National Strategy for Artificial Intelligence 2031.

"This policy marks a significant milestone in the Center's journey to realize Dubai's annual plan, accelerating the adoption of AI applications and technologies in line with the directives of His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai, Deputy Prime Minister and Minister of Defence, and Chairman of the Executive Council of Dubai. It serves as a cornerstone in supporting the roadmap to enhance the quality of life in Dubai by integrating AI across all vital sectors, aligning with the goals of the Dubai Economic Agenda (D33), which aims to double Dubai's economy over the next decade and position it among the top three global economic cities," added Al Shaibani.

Qualitative Addition

His Excellency Amer Sharaf, CEO of the Cybersecurity Systems and Services Sector at the DESC, highlighted that this policy is a new qualitative addition to the suite of innovative projects and policies launched by the Center. It comes as part of its mission to create a safe and reliable cyberspace that supports Dubai's digital infrastructure, reinforcing the Emirate's vision to strengthen its global leadership in cybersecurity.

This initiative plays a vital role in boosting trust, fostering the growth and development of AI technologies, and solidifying Dubai's position as a global hub for AI. It also aims to protect innovations from cyber threats, enhance cooperation between the public and private sectors, and attract AI investments to the Emirate.

By launching this groundbreaking initiative and participating in the event as an official partner, the Center seeks to stay ahead of the rapidly growing use of AI technologies across various sectors. AI has become a foundational pillar for driving innovation and building a knowledge-based economy and society. To this end, the Center is committed to establishing clear and precise security standards that ensure the safe and responsible use of AI technologies, including generative AI models, safeguarding them from cybersecurity risks.

The event saw the participation of over 5,000 business leaders from 100 countries, 500 investors, and around 100 exhibitors, all gathered to explore the latest developments in AI, Web3, and digital economies. These efforts are part of the Center's initiatives to support the national efforts aimed at strengthening Dubai's position as a global hub for innovation, stimulating economic growth, and building a safer, more sustainable future.

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

STAYING AHEAD OF THREATS

SERTAN SELCUK, VP FOR METAP & CIS, OPSWAT TELLS ANITA JOSEPH HOW GOVERNMENT ORGANISATIONS CAN SAFEGUARD AGAINST THREATS AND THE BEST PRACTICES TO BE FOLLOWED.

What are the threats government organisations face? Government organisations face many threats due to the sensitive data they handle and the critical services they provide. These threats come from state actors, hacktivists, and criminal organisations, each with distinct motivations and capabilities. State actors, often foreign governments, engage in cyber espionage to gather intelligence or disrupt operations, leveraging substantial resources for sophisticated attacks. Hacktivists target government systems to promote political or ideological causes, utilising methods like data leaks and denial-of-service attacks. Cybercriminals seek financial gain through ransomware, data theft, and fraud, exploiting vulnerabilities in government systems.

Insider threats, from employees or contractors with access to sensitive information, pose a significant risk through both intentional and unintentional actions. Additionally, terrorist organisations may target government infrastructure to cause disruption and fear, impacting national security and public safety. Supply chain attacks, where external vendors and contractors are compromised, provide indirect routes for infiltrating government systems. Compounding these threats is the cybersecurity skills shortage, which hampers the ability of government agencies to defend against these varied threats, making it challenging to implement and maintain comprehensive security measures. The complexity and variety of these threats, along with the strategic importance of government institutions, make them high-priority targets for a wide range of malicious actors.

How can government organisations safeguard from threats?

Government organisations can safeguard against threats by implementing comprehensive cybersecurity protections. At a tactical level, it is essential for these organisations to understand and develop a program and processes that align with industry cybersecurity frameworks. This alignment ensures that the diverse types of data flowing in and out of their systems are secured and safe. Utilising compliance guides the implementation of appropriate tools and supports continuous monitoring and improvement of cybersecurity measures.

However, it is crucial to avoid the pitfall of relying on a single tool to address all security needs. Effective cybersecurity requires a coordinated ecosystem that includes people, processes, and technology working together. Simplifying this ecosystem, where possible, is beneficial but recognising that no single solution can address all threats is vital. Ensuring the integration and cooperation of information technology and operational technology environments is also important.

What are the best practices to be followed?

One crucial practice is scanning all incoming data for viruses and potential zero-day threats, regardless of its source—be it the cloud, peripheral media, email, or other channels. Additionally, detecting the country of origin for incoming data is essential to assess and mitigate potential risks associated with specific regions.

Given the complexity of federal government networks, implementing cross-domain solutions is also critical. These solutions address the need for secure data flow across networks with varying trust levels. Ensuring a one-way, proven data flow helps maintain the integrity and security of sensitive networks by verifying that incoming data is both authorized and safe. Securing the supply chain is another important best practice. Government organisations must rigorously vet their vendors and partners to prevent vulnerabilities from being introduced through third-party products and services.

How can governments prioritise collaboration, standardisation, and technology adoption to fortify critical infrastructure against cyber threats effectively? Way forward for 2024?

The government can prioritise collaboration, standardisation, and technology adoption by focusing on several key areas. First, fostering collaboration among UAE government agencies, private sector partners, and international allies is crucial for sharing threat intelligence, best practices, and resources. This collaborative approach enhances the collective ability to detect, prevent, and respond to cyber threats.

TECHNOLOGY ADOPTION, PARTICULARLY WITH AI AND MACHINE LEARNING, IS ESSENTIAL FOR STAYING AHEAD OF EVOLVING CYBER THREATS.

Standardisation plays a pivotal role in ensuring a unified and consistent approach to cybersecurity. Adopting widely recognised frameworks such as the National Institute of Standards and Technology (NIST) guidelines, alongside UAE-specific regulations like the UAE Information Assurance Standards (UAE IAS), helps create a foundation for security measures across various sectors. These standards guide organisations in implementing best practices and maintaining a high level of security.

Technology adoption, particularly with AI and machine learning, is essential for staying ahead of evolving cyber threats. AI and machine learning can enhance the ability to detect and respond to threats quickly and efficiently. However, these technologies also present new challenges, as adversaries can exploit them to launch sophisticated attacks. Therefore, it is crucial to continuously develop and refine AI-driven cybersecurity solutions to ensure they remain effective in countering advanced threats.

Looking ahead to 2024, the way forward for the UAE involves leveraging AI and machine learning, both as defensive and offensive tools. While these technologies pose significant threats due to their potential for automating attacks without human intervention, they also offer powerful capabilities for detecting and mitigating those very threats. The focus must be on staying ahead in the race to utilise AI effectively for cybersecurity.

Additionally, compliance and regulatory mandates help ensure all public sector entities adhere to stringent cybersecurity standards. Although creating these regulations can be relatively straightforward, implementing them can be challenging. Therefore, the government must provide the necessary support and resources to facilitate compliance.

SECURING TELCOS WITH QUANTUM-SAFE NETWORKS IN THE MIDDLE EAST

STEFANO RESI, HEAD OF STRATEGY & EXECUTION FOR NETWORK INFRASTRUCTURE, NOKIA MIDDLE EAST AND AFRICA

The requirement for safe and trusted digital infrastructure is more important than ever in the linked world of today. The region's ambitious digital transformation initiatives, like Saudi Arabia's Vision 2030 and the UAE's National Innovation Strategy, are driving significant growth and technological advancements. However, with these advancements come new vulnerabilities, emphasizing the need for enhanced security measures.

Digitalisation introduces a double-edged sword: while it fosters agility and accessibility, it also expands the attack surface. With the potential to completely transform industries like materials science, artificial intelligence, and medicine, quantum computing poses a serious threat to established cybersecurity practices. The availability of Cryptographically Relevant Quantum Computers (CRQCs), often known as "Q-day," are a real threat because they can break the encryption systems that are in place to protect our vital infrastructure.

Quantum-Safe Networks (QSN): Multi-Layered Defence-in-depth

Quantum-Safe Networks (QSNs) provide critical infrastructure operators in the government, defence, banking, healthcare, and power utility sectors, along with telecommunication service providers, with a multi-layered defence strategy that strengthens security and trust. By layering obstacles in the way of potential attackers, this strategy offers supplementary network layer cryptographic protection to application layer security, ensuring cryptographic resilience and help to manage the risk of compromise.

Strengthen Your Network Security Now

While some may view quantum threats as a concern for the distant future, the "harvest now, decrypt later" (HNDL) tactic employed by threat actors exposes a critical vulnerability. These actors are currently collecting encrypted data, confident that they will be able to decrypt it once CRQC technology becomes available. Thus, the imperative to implement QSNs is immediate. Transitioning to quantum-safe cryptography and adopting a defence-in-depth strategy requires proactive planning with a defined roadmap. By initiating this process now, organisations can manage their risk profiles, build cryptographic resilience, and protect sensitive information before it's too late.

The Middle East has already started embracing quantum-safe technologies. For instance, the UAE is at the forefront of adopting advanced security measures to protect its digital infrastructure. In March of this year, the UAE Cyber Security Council and CPX Holding released the "State of the UAE - Cybersecurity Report 2024", which highlighted the cyber threat landscape facing the UAE, identifying over 155,000 vulnerable assets within the UAE, with more than 40 percent of critical vulnerabilities remaining unaddressed for over five years.

Ensuring Quantum-Safe Connectivity

Achieving quantum-safe connectivity requires a comprehensive strategy. Nokia's crypto-resilient defence-in-depth approach involves multi-layered network cryptography tailored to specific business and use case needs. This strategy ensures the scalability of quantum-safe network deployment and adaptability to the evolving quantum landscape. It necessitates the implementation of security measures both complementarily and cumulatively across various layers (application, network, connectivity, and potentially future quantum-safe application layers).

At the core of this strategy are quantum-safe cryptographic keys based on both mathematical and physical principles, along with appropriate key distribution. Complementing this foundation, AES256 network encryption provides multiple layers of IP and optical cryptography, enhancing application-level cryptography for secure quantum-safe connectivity. Nokia Bell Labs leads cutting-edge research in specific technological domains, driving innovation and shaping the future of quantum-safe network solutions.

QUANTUM-SAFE NETWORKS PROVIDE CRITICAL INFRASTRUCTURE OPERATORS A MULTI-LAYERED DEFENCE STRATEGY THAT STRENGTHENS SECURITY AND TRUST.

Harnessing the Power of Collaboration

Collaboration is essential: Nokia partners with industry experts, including areas such as Quantum Key Distribution (QKD) and specialists in Public Key Infrastructure with Post-Quantum Cryptography (PKI-PQC). These partnerships form the foundation of the QSN strategy, uniting diverse entities in the pursuit of a resilient, future-proof, secure communication infrastructure to protect customers' networks.

Embracing the Quantum Leap

Relying on a single encryption layer at the application layer is no longer sufficient. We require a crypto-resilient, multi-layer, adaptable defence-in-depth approach to counter the evolving threats posed by quantum computing. Implementing QSN fortified with quantum-safe cryptographic techniques is imperative. This multi-faceted solution spans various network infrastructure layers, providing a defence-in-depth approach that ensures adaptable and scalable digital communication across the application and networking layers, and complementary with evolving advancements in quantum-safe cryptography for the application layer.

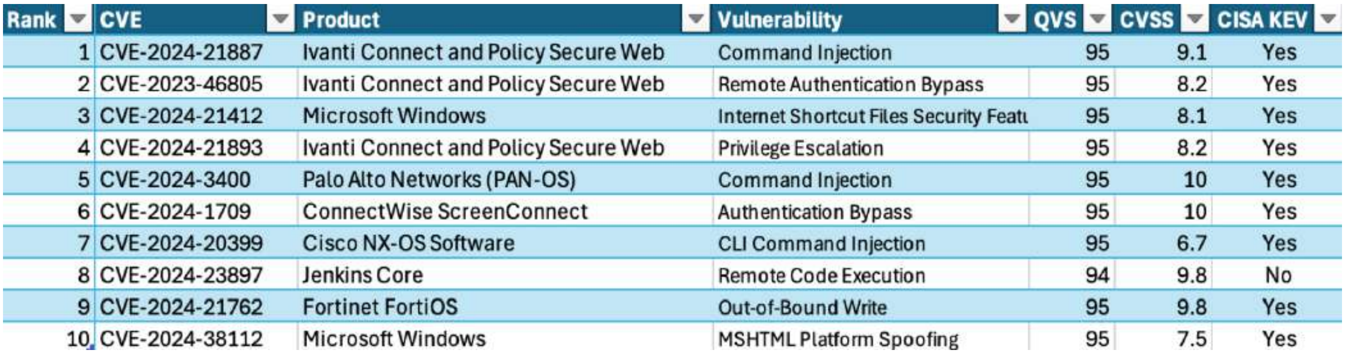
By safeguarding the trust and security of our digital communications infrastructures, we can ensure data integrity, security, and privacy in the quantum era. To achieve this, we must act now to manage the risk to our global digital economies and societies by planning and deploying Quantum-Safe Network solutions today. This proactive approach is crucial across all mission-critical markets, including those in the Middle East. Telecom service providers in the region can offer quantum-safe private or managed infrastructure to these markets, laying the groundwork for future incremental quantum-safe monetisation.

COMMON VULNERABILITIES AND EXPOSURES RISE BY 30% IN 2024: QUALYS THREAT RESEARCH UNIT

According to new research from the Qualys Threat Research Unit (TRU), between January to mid-July, the CVE count rose by 30% from 17,114 in 2023 to 22,254 in 2024. The increase in CVEs reflects rising software complexity and the broader use of technology, necessitating advanced and dynamic vulnerability management strategies to mitigate evolving cybersecurity threats.

A thorough analysis of the 22,254 reported vulnerabilities during the initial seven and a half months of 2024 (up until the research cut-off date of July 21, 2024) reveals that a precise subset of 0.91% (almost 1%) has been weaponized, and a very small fraction accounts for the most severe threats. This subset represents the highest risk, characterised by weaponised exploits, active exploitation through ransomware, threat actors, malware, or confirmed wild exploitation instances.

The analysis also indicates an increase in the weaponisation of old CVEs since the onset of 2024. Over the last 7.5 months, there has been a notable increase, slightly over 10%, in the weaponisation of older CVEs identified before 2024, which is a stark reminder that cybersecurity is not just about staying ahead but also about not falling behind. Some of these vulnerabilities have been trending on



Rank	CVE	Product	Vulnerability	QVS	CVSS	CISA KEV
1	CVE-2024-21887	Ivanti Connect and Policy Secure Web	Command Injection	95	9.1	Yes
2	CVE-2023-46805	Ivanti Connect and Policy Secure Web	Remote Authentication Bypass	95	8.2	Yes
3	CVE-2024-21412	Microsoft Windows	Internet Shortcut Files Security Featu	95	8.1	Yes
4	CVE-2024-21893	Ivanti Connect and Policy Secure Web	Privilege Escalation	95	8.2	Yes
5	CVE-2024-3400	Palo Alto Networks (PAN-OS)	Command Injection	95	10	Yes
6	CVE-2024-1709	ConnectWise ScreenConnect	Authentication Bypass	95	10	Yes
7	CVE-2024-20399	Cisco NX-OS Software	CLI Command Injection	95	6.7	Yes
8	CVE-2024-23897	Jenkins Core	Remote Code Execution	94	9.8	No
9	CVE-2024-21762	Fortinet FortiOS	Out-of-Bound Write	95	9.8	Yes
10	CVE-2024-38112	Microsoft Windows	MSHTML Platform Spoofing	95	7.5	Yes

the dark web for months. An example is CVE-2023-43208 NextGen Mirth Connect Java XStream (Qualys Vulnerability Score 95/100), which heavily involves systems used by healthcare organisations.

"This resurgence of previously identified vulnerabilities, which mainly impact remote services and public-facing applications, highlights a significant oversight in updating and enforcing cybersecurity protocols. It emphasises the need to shift from a purely reactive security posture to a more proactive, predictive, and preventative approach," commented Saeed Abbasi, Product Manager, Vulnerability Research at Qualys TRU. "By adopting a holistic view that incorporates continuous monitoring, rapid patch management, and a deep understanding of the evolving threat landscape, businesses can significantly reduce their vulnerability to cyberattacks. This strategic foresight will protect critical assets and foster trust and resilience in our increasingly interconnected world."

Mid-2024's Most Wanted: Top 10 Exploited Vulnerabilities

In 2024, a select group of vulnerabilities have emerged as particularly prevalent targets for cyberattacks. Qualys ranks vulnerabilities based on their prevalence and impact, integrating multiple factors such as CVSS base scores, exploit code maturity, real-time threat indicators, and evidence of active exploitation, among others, for a comprehensive assessment.

This Top 10 ranking reflects their current significance in the cyber threat landscape. This designation is derived from an analysis incorporating data from over 25 distinct threat intelligence sources utilised by Qualys.

Critical Contenders: Just Missed the Cut

While the top 10 list captures the most crucial vulnerabilities of mid-2024, a few just missed the cut but demanded attention due to their high severity and potential impact. These vulnerabilities are critical for organizations to address immediately.

- **CVE-2023-22527 (Atlassian Confluence):** This severe remote code execution vulnerability, with a QVS of 95 and a CVSS score of 9.8, allows attackers to run arbitrary code on affected installations.

- **CVE-2023-48788 (FortiClient EMS):** This SQL injection flaw, which scores a QVS of 95 and a CVSS of 9.8, poses a high risk by allowing attackers to manipulate databases and access sensitive information.

- **CVE-2024-24919 (Check Point Security Gateways):** This information disclosure vulnerability, although it has a slightly lower CVSS score of 8.6, and a QVS of 95, can leak sensitive data.

All of the above vulnerabilities are listed on the CISA KEV, highlighting their recognised significance, exploitation in the wild, and potential impact. While not included in the top 10, each presents a clear and present danger to network security and requires prompt attention from cybersecurity teams to mitigate risks effectively and protect sensitive systems.

"Adopting a hybrid vulnerability management strategy that combines agent-based and agent-less methods, including network, external, and passive scans, is crucial. This approach is particularly pertinent given that 21.74% of CVEs in the CISA KEV catalog are actively exploited on network and perimeter devices, underscoring the need for a comprehensive security posture to effectively identify and mitigate vulnerabilities. Organisations must ensure regular updates, diligent patch management, and advanced threat detection systems are in place to mitigate the risks associated with high-critical vulnerabilities," added Abbasi.

ADOPTING A HYBRID VULNERABILITY MANAGEMENT STRATEGY THAT COMBINES AGENT-BASED AND AGENT-LESS METHODS, INCLUDING NETWORK, EXTERNAL, AND PASSIVE SCANS, IS CRUCIAL.

WITH AI ADOPTION IN THE MIDDLE EAST PROJECTED TO CONTRIBUTE OVER $320 BILLION TO THE REGION'S ECONOMY BY 2030, SECURING THESE TECHNOLOGIES IS NO LONGER OPTIONAL BUT ESSENTIAL.

TRENDMICRO AND NVIDIA ACCELERATE AI SECURITY WITH TREND VISION ONE AND NVIDIA NIM INTEGRATION

Trend Micro Incorporated, a global leader in cybersecurity solutions, recently announced a strategic partnership with NVIDIA to enhance the security of AI-driven private data centers across regional and global markets. This collaboration is a key part of Trend Micro's broader initiative to advance AI implementation for enterprises and governments, marking a significant step forward in securing AI technologies. By integrating NVIDIA NIM microservices into Trend Micro's Vision One™ Sovereign Private Cloud—a key component of the NVIDIA AI Enterprise software platform—this solution enables organisations to harness AI's transformative potential while maintaining robust security and long-term business resilience.

As organisations navigate the complexities of adopting generative AI, minimising risks at every level is critical. Trend Micro is focused on understanding infrastructure changes, user behaviors, and operational needs to protect data against both known and unknown risks at every stage of adoption in this new technological era. Recognising this, Trend Micro and NVIDIA are jointly developing strategies to ensure the secure and sustainable integration of AI technologies. By focusing on strategic foresight and avoiding the risks associated with shortsighted implementations, such as misconfigurations and data breaches, this partnership empowers organisations to fully harness AI's benefits without compromising operational integrity.

"With AI adoption in the Middle East projected to contribute over $320 billion to the region's economy by 2030, securing these technologies is no longer optional but essential," said Dr. Moataz Bin Ali, Regional Vice President and Managing Director, MMEA, Trend Micro. "With the integration of NVIDIA NIM microservices into our Trend Vision One Sovereign Private Cloud, we are setting a new standard for AI security. This initiative not only fortifies our customers defences but also empowers them to harness the full potential of AI with unparalleled confidence. Our commitment is to lead the industry in delivering innovative, resilient solutions and driving forward the future of secure AI technology".

The collaboration between Trend Micro and NVIDIA encompasses NVIDIA AI Enterprise, NVIDIA NIM microservices, and the NVIDIA Morpheus cybersecurity framework. This suite of solutions addresses the urgent needs of enterprises, governments, and critical infrastructure organisations seeking reliable partners for AI implementation and operations. Trend Vision One Companion, an AI assistant powered by NVIDIA NIM microservices and accelerated computing, delivers proactive threat detection, rapid response, and sensitive data protection, even in isolated environments, thereby enhancing productivity and response efficiency.

Furthermore, Trend Vision One customers leveraging NVIDIA Morpheus experience advanced extended detection and response (XDR) capabilities, enabling superior processing and classification of extensive data volumes for quicker threat detection and anomaly identification. This approach reduces noise and builds detailed behavioral fingerprints, allowing analysts to focus on critical events. Additionally, organisations with stringent data sovereignty requirements, such as governments and critical infrastructure entities, can safely deploy AI with Trend Vision One's Sovereign and Private Cloud integration, facilitated by NVIDIA NIM microservices, ensuring security without sacrificing control.

This strategic partnership between Trend Micro and NVIDIA represents a pivotal advancement in the security landscape, providing organisations with the tools needed to navigate the complexities of AI technology while maintaining robust security and operational resilience.

KASPERSKY DISCLOSES FRAUDULENT CAMPAIGNS DURING BACK-TO-SCHOOL SEASON

As the back-to-school season has begun in full swing, Kaspersky's cybersecurity experts have detected a significant surge in fraudulent activities. Every year, cybercriminals exploit the busy period of academic preparations and purchases, launching sophisticated phishing campaigns. However, Kaspersky experts warn that this year, the campaigns have become more targeted, specifically aiming to steal personal data from students, educators, and administrators in the educational sector.

Fraudsters are increasingly leveraging data collection forms on platforms like SurveyHeart.com, a questionnaire like Google Forms, to carry out scams.

In one such scheme - phishing attack that targets students at Neumann University in the U.S. - victims receive a notification claiming they are using two different Microsoft school emails across various university portals. To prevent their Office 365 account from being deactivated, they are asked to complete a survey requiring sensitive details such as their name, phone number, university email, and account password.

Another scam uncovered by Kaspersky experts involves fraudsters creating fake giveaways that promise students a chance to win various high-end gadgets useful for education, from iPhones to iPads and laptops. To enter these enticing contests, victims are asked to provide personal information and are instructed to provide personal information and indicate their preferred laptop model. Additionally, individuals are prompted to share a link to a prize-draw page with 15 contacts via WhatsApp. While the prospect of winning a valuable item like a laptop is the lure, there's a hidden catch: the so-called winners are told they must pay for the delivery of their prizes. This demand for additional payment is a clear red flag that the giveaway is a scam.

The offer may seem tempting, but the combination of an unusually generous prize and the requirement to cover delivery costs is a telltale sign of fraudulent activity.

To stay safe against education fraud, Kaspersky experts also recommend:

- Stay Skeptical: Exercise caution when encountering "too good to be true" offers, especially if they require payments or personal information upfront.
- Verify the Source: Thoroughly research any scholarships, giveaways, or offers that come your way. Look for official contact details and confirm legitimacy before taking any action.
- Secure Your Information: Avoid sharing sensitive data online unless you're absolutely certain about the legitimacy of the request.
- Use Trusted Sources: Stick to official school websites, recognized scholarship platforms, and reputable retailers when making payments or providing personal information.
- Enable Multi-Factor Authentication (MFA): Activate MFA wherever possible, adding an extra layer of security to your online accounts. Use a reliable Password manager that doesn't just store your passwords but also generates one-time passwords for 2FA automatically.
- Use a reliable security solution for comprehensive protection from a wide range of threats, such as Kaspersky Premium.

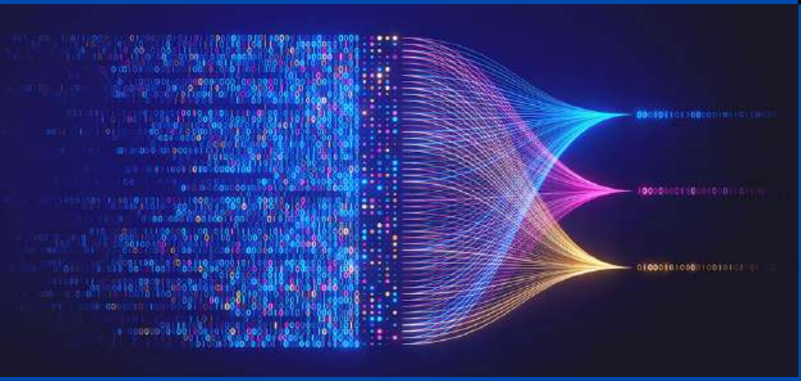
CLOUD BOX
TECHNOLOGIES

Great Place To Work.
Certified
AUG 2024-AUG 2025
UAE

EMBRACE DIGITAL TRANSFORMATION

SHEILD YOUR BUSINESS AGAINST CYBERATTACKS

ACCELERATE. INNOVATE. SCALE. AI.



MAKE YOUR MOVE TO THE CLOUD

Visit Us!	Our Office:	Call Us!
www.cbt.ae	#3807, Latifa Tower - Sheikh Zayed Rd - Trade Centre - Trade Centre 1 - Dubai, AE	04 210 1900

Meet Us!
GITEX GLOBAL
14 - 18 October