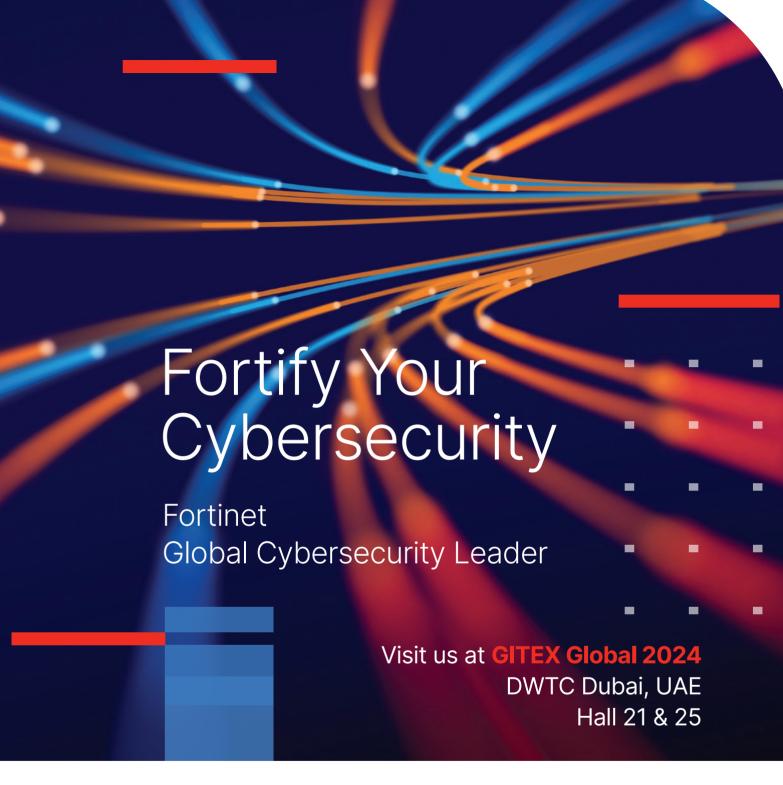
ISSUE 88 | OCTOBER 2024 WWW.TAHAWULTECH.COM

SECOND ADVISOR NIDDLE EAST

TRANSFORMING CYBER DEFENCE

MERIAM EL OUAZZANI, SENIOR REGIONAL DIRECTOR, MIDDLE EAST, TURKEY AND AFRICA AT SENTINELONE, SPEAKS TO ANITA JOSEPH ABOUT PURPLE AI AND HOW IT IS TRANSFORMING NEW-AGE SECURITY.



The Fortinet Security Fabric is the industry's highest-performing cybersecurity platform, delivering broad, integrated, and automated cybersecurity capabilities supported by a large, open ecosystem. The Fortinet Security Fabric empowers organizations to achieve secured digital acceleration outcomes by reducing complexity, streamlining operations, and increasing threat detection and response capabilities.

Learn more at fortinet.com



CONTENTS

Securaty





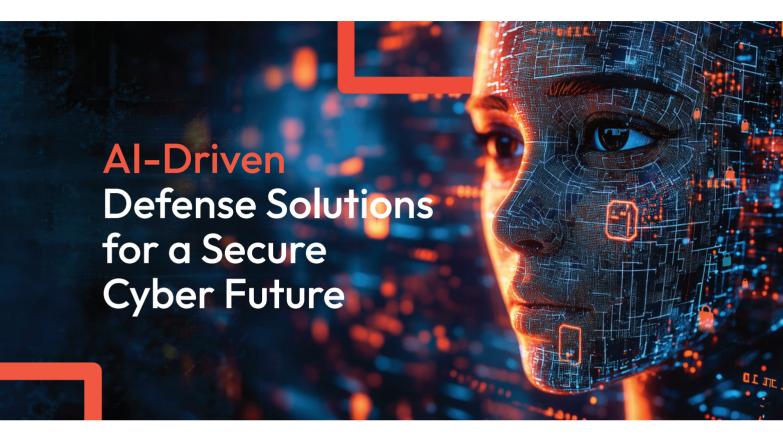




- News from the cybersecurity world in the region and beyond.
- Alexey Potapov, Attack Detection
 Department Expert, PT Expert Security
 Center at Positive Technologies, on how
 behavioral analytics are changing the rules
 of the game.
- Sakkeer Hussain, Director Sales & Marketing at D-Link Middle East & Africa, on how the company is committed to a safer, more secure network ecosystem with its cutting-edge security tools and solutions.
- Rohan Daniel Nair, Founder & Chief Operating Officer at AHAD, on how the company combines innovation & technology to offer proactive defence solutions against the most sophisticated threats.







Visit us at Hall 1 #H1-A20





Cyber, Cloud & Network Infrastructure





EDITOR'S NOTE



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

> Anita Joseph Editor

FVFNTS





GITEX 2024: A SPOTLIGHT ON INNOVATION IN SECURITY TECHNOLOGY

s the global technology landscape evolves, GITEX 2024 promises to be a vibrant hub for innovation, excellence. and visionary ideas, particularly in the realm of cybersecurity.

GITEX stands as a beacon for technology enthusiasts, industry leaders, and innovators, gathering security frontrunners and visionaries from around the world. As businesses increasingly face complex cybersecurity threats, the event will highlight cutting-edge **FUTURE OF** solutions and technologies **SECURITY** designed to safeguard digital assets and ensure compliance in an everchanging landscape.

Attendees can expect to witness groundbreaking advancements in artificial intelligence, machine learning, and data analytics, all tailored to bolster security frameworks. Leading firms will showcase their latest innovations, demonstrating how these technologies can preemptively address vulnerabilities and enhance threat detection and response capabilities.

In addition to showcasing products, GITEX will host insightful discussions and panels featuring industry superstars. These sessions will delve into pressing security challenges, regulatory landscapes, and the future of cybersecurity, offering invaluable perspectives from those at the forefront of the industry.

The event also serves as a unique networking opportunity, fostering

> connections between startups and established enterprises. encouraging collaboration that drives forward-thinking

solutions.

As GITEX 2024 approaches, it is clear that this year's gathering will not only spotlight the latest in security technologies but also inspire a collective vision for the future of cybersecurity. With innovation and excellence at its core, GITEX is set to redefine how we perceive and implement security in our increasingly digital world. Join us as we embark on this journey into the future of technology!

FOUNDER, CPI ominic De Sousa (1959-2015)

Published by



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

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com

Editor Anita Joseph anita.joseph@cpimediagroup.com

Online Editor

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, UAF

Tel: +971 4 5682993

© Copyright 2024 CPI All rights reserved

COMMVAULT TO SHOWCASE INDUSTRY-LEADING CYBER RESILIENCE SOLUTIONS AT GITEX GLOBAL 2024

Commvault, a leading provider of cyber

resilience and data protection solutions for the hybrid cloud, is set to demonstrate industry-leading solutions and offerings at GITEX GLOBAL 2024, the premier technology event in the Middle East.

At this year's event, Commvault will unveil its latest advancements in cyber resilience, underscoring the critical importance for organisations to implement cutting-edge technologies to ensure protection and efficiency. With a specific focus on Commvault Cloud Cleanroom Recovery, the organisation will be showcasing how they have turned the concept of cleanrooms on its head and that their comprehensive portfolio has never been more relevant and more necessary to the industry than they are today.

At GITEX 2024, Commvault will demonstrate how its offerings are tailored to meet the unique needs of businesses in the UAE, Saudi Arabia and the wider Middle East and North Africa region, providing unparalleled protection and recovery capabilities. Visitors at GITEX 2024 can expect to see displays of Commvault's latest innovations, including advanced data protection, cloud integration and Aldriven automation.

"In today's digital landscape, cyber resilience is not just a tech concern but a business imperative," said Fady Richmany, Regional Vice President & General Manager, Emerging Markets, CEE, CIS & META at Commvault. "Our solutions are designed to empower businesses to stay ahead of threats and



ensure continuity by helping customers cementing a Cyber Recovery strategy to defend against Al-driven, systematic, pervasive cyber-attacks. Looking ahead, Commvault is committed to continuing its legacy of providing the gold standard in cyber resilience. We look forward to attending GITEX, the premier technology event in the region, to discuss this and more with our customers, partners and industry experts," added Richmany.

WSO2 TO DEMONSTRATE 'FOUNDATIONAL TECHNOLOGIES' FOR DIGITAL TRANSFORMATION AND SECURE CLOUD MIGRATION AT GITEX

WS02, the global leader

in digital transformation technology, has announced its participation at the forthcoming GITEX Global 2024, where it will exhibit under the theme "Foundational technologies to create awesome digital experiences".

As attendees at GITEX

Global air the technology industry's most pressing issues, WSO2 will offer its unique expertise on how to leverage technology to create digital experiences quickly, easily and securely. The company will showcase its latest advancements in API management and integration, including Choreo, its internal developer platform that redefines

how DevOps teams create digital



experiences. It will also demonstrate its customer identity access management (CIAM) capabilities at a time when IBM estimates the average cost of a data breach in the Middle East at US\$8.7 million.

As a channel focused organisation,

WS02 will also look to strengthen its partnerships at GITEX and expand its market reach. "GITEX is a global event that attracts a wide range of technology stakeholders, including potential partners, customers, and investors," said Uday Shankar Kizhepat, Vice President and General Manager - Middle East and Africa Region, WSO2. "This is an opportunity for us to forge new relationships and expand our presence throughout the

MEA region. We onboard two partners each year to give them exposure to GITEX through WSO2. This year we have partnered with 3Pillars Digitalization and Aujas, and we'll also be introducing a new partner, Systems Ltd., at the event."

6 OCTOBER 2024 www.tahawultech.com

CLOUDFLARE TO SHOWCASE CLOUD FOR THE "EVERYWHERE WORLD" AT GITEX 2024

Cloudflare Inc., the leading connectivity

cloud company, has announced its participation at GITEX 2024, the premier technology event in the Middle East, taking place from October 14 to 18 at the Dubai World Trade Centre. Cloudflare will present its latest suite of products and solutions that help businesses regain control of their technology and security environments, by reducing complexity and improving visibility across their onpremises, public cloud, SaaS and public Internet domains.

At GITEX 2024, Cloudflare will demonstrate how its technologies are reshaping the landscape of digital infrastructure and security. The company will spotlight the connectivity cloud, a state-of-the-art solution designed to enhance connectivity and optimise performance for enterprises across

the globe. This AI enabled platform offers unparalleled visibility, reliability, security, privacy and speed by leveraging Cloudflare's extensive global network that spans 330 cities in over 120 countries.

Bashar Bashaireh, RVP Middle East and Türkiye at Cloudflare, commented on the company's commitment to the region: "Today, everything needs to be connected to everything everywhere, all the time. This hyperconnectivity creates new challenges related to security, performance, resilience and privacy. As the world's first connectivity cloud, Cloudflare helps connect and protect millions of customers globally. Everyone from individuals to the world's largest enterprises use our unified platform of networking, security, and developer services to succeed in the everywhere world."

"The Middle East is experiencing



rapid digital transformation, and we are proud to be at the forefront of this evolution. Cloudflare's solutions are designed to meet the unique challenges faced by enterprises in this region, providing them with the tools they need to achieve secure, reliable, private and high-performance connectivity. Our participation at GITEX 2024 underscores our dedication to supporting Middle Eastern businesses as they navigate the complexities of today's digital landscape," Bashaireh continued.

NUTANIX TO SHOWCASE CLOUD INNOVATIONS AT GITEX 2024 WITH THEME 'EXPERIENCE CLOUD FREEDOM'

Nutanix, a leader in hybrid multicloud

computing, has announced its participation in GITEX 2024, taking place between 14 - 18 October at the Dubai World Trade Centre. This year, Nutanix will highlight its commitment to delivering cloud freedom through innovative solutions, including strategic partnerships and groundbreaking technologies.

Raif Abu Diab, Country Manager
- South Gulf & Sub-Saharan Africa
at Nutanix comments, "Nutanix is
dedicated to helping customers
accelerate their digital transformation.
Our solutions simplify the deployment
and management of hybrid multi-cloud
infrastructures, ensuring scalability,
flexibility, and cost efficiency. We are
committed to supporting organisations in
navigating today's digital-first world."



"GITEX is a crucial platform for us to connect with the vibrant technology community in the Middle East. We look forward to showcasing our latest innovations, strengthening relationships with customers and expanding our ecosystem by building on current partnerships and forging new connections with local technology firms, cloud providers, and channel partners."

Nutanix will be exhibiting at Hall 6, stand #C10 for the ninth consecutive year, welcoming alliances and partners from across the Middle East to share a unified go-to-market message. The goal is to demonstrate how its full stack of solutions addresses the IT challenges faced by organisations today. As part of its alliance strategy, Nutanix is keen to showcase its collaboration with Dell Technologies to deliver new joint solutions that enhance hybrid cloud strategies for customers. This partnership reinforces Nutanix's mission to provide comprehensive, customercentric solutions that address the diverse needs of the market.

www.tahawultech.com OCTOBER 2024

FORTINET ANNOUNCES PROGRESS TOWARDS MISSION TO TACKLE CYBERSECURITY SKILLS SHORTAGE

Fortinet, the global cybersecurity leader

driving the convergence of networking and security, has announced significant progress in its mission to address the cybersecurity skills shortage through its Training Institute programs. As part of the company's commitment to closing the cyber workforce gap, Fortinet pledged to train 1 million people in cybersecurity by the end of 2026 and through the Fortinet Training Institute programs has achieved significant strides toward this goal. With more than half a million people having been trained since the 5-year span pledge was announced. Fortinet is on track to meet this commitment by the end of 2026.

John Maddison, Chief Marketing

Officer at Fortinet said, "Through our longstanding investments to address the cyber talent shortage, Fortinet continues to grow and expand our programs and strategic partnerships by delivering an award-winning cybersecurity training and certification program. Addressing the cyber skills gap is vital to enhancing our society's collective cyber resiliency and we are committed to developing the current and future cyber workforce through the Fortinet Training Institute. As part of this effort, we remain focused on our pledge to train 1 million individuals in cyber by 2026."

As the cybersecurity landscape grows increasingly complex, the demand for



skilled professionals continues to grow with an estimated 4.8 million cybersecurity professionals required to address the industry's workforce gap. At the same time, Fortinet's 2024 Global Cybersecurity Skills Gap Report reveals that 70% of organisations believe the shortage of skilled cybersecurity professionals is increasing risks to their security.

MINDWARE SIGNS VAD PARTNERSHIP WITH ASSURED DATA PROTECTION IN THE MIDDLE EAST

Mindware, a leading value-added

distributor (VAD) in the Middle East and Africa, has signed a strategic distribution partnership with Assured Data Protection (Assured), the prominent IT managed services provider (MSP) for cloud data protection solutions. This collaboration will benefit partners and businesses across the region, providing them with cutting-edge backup and cyber recovery services as managed services at affordable prices.

Through this partnership, Mindware will work with Assured to offer its customers, MSPs, and resellers comprehensive solutions to ensure that businesses can protect and recover their critical data and operations in the event of outages, natural disasters, ransomware, and cyber-attacks. Assured customers and partners receive a fully managed Rubrik service from design and implementation through to recovery and daily proactive support. Rubrik's Zero Trust Data Security helps organisations



Ehab Adel, Business Unit Manager at Mindware (L) and Rob Mackle, EMEA Managing Director at Assured Data Protection (R)

achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications.

Ehab Adel, Business Unit Manager at Mindware, expressed enthusiasm about the partnership: "We are thrilled to partner with Assured, the first and largest Rubrik MSP, to deliver an unparalleled 24/7/365 managed service that guarantees robust cyber resilience for our channel partners. This strategic alliance greatly strengthens

our data protection and managed services portfolio, reinforcing our position as a key player in helping organisations swiftly recover from cyber threats, including ransomware. With Assured, we can now provide a more flexible and cost-effective approach to deploying Rubrik solutions for businesses of all sizes."

Rob Mackle, EMEA Managing
Director at Assured Data Protection,
commented, "Rubrik offers an outstanding
immutable cyber recovery technology,
combined with our industry leading
24/7/365 managed service. We're excited
to deliver our innovative disaster recovery
solutions through Mindware's channel
partners to every business that needs it
in the Middle East. We see Mindware as a
great partner to help establish our brand
in the region. Our launch into the Middle
East is another important step forward in
our ambitious growth plans for 2024 and
beyond," he added.

8 OCTOBER 2024 www.tahawultech.com

D-Link



Experience Next-Generation 5G Connectivity

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



Higher Speed



Lower Latency



Larger Capacity

Plug & Play, Enjoy Fast Connectivity Where You Need



Easy Setup & Manage











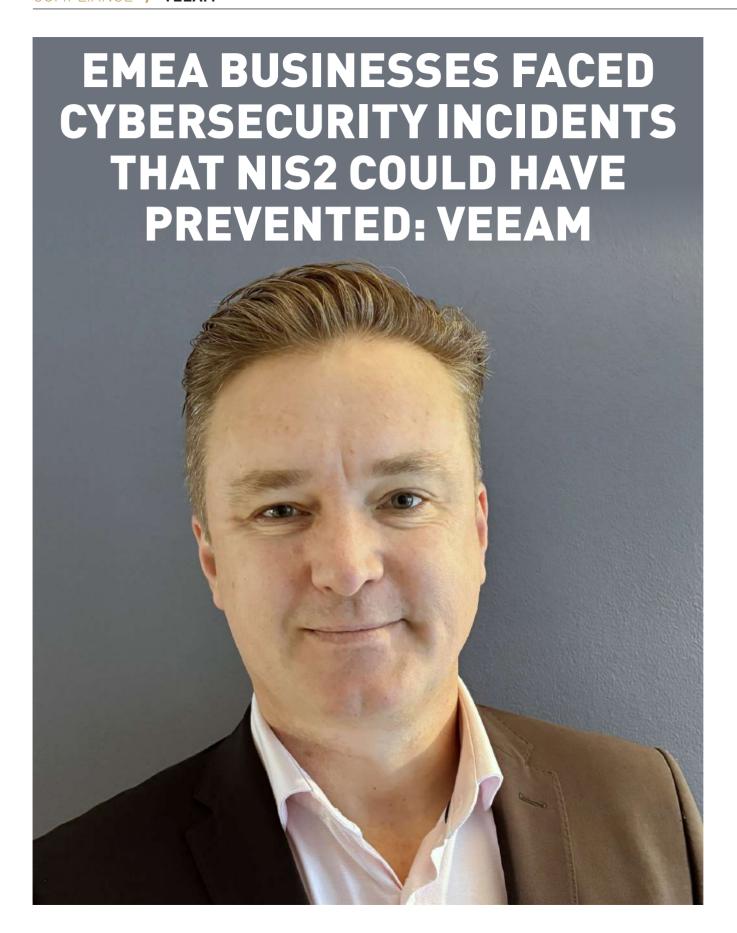


G530

5G NR AX3000 Wi-Fi 6 Router

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





rganisations are navigating a landscape of mixed emotions as the Network and Information Security Directive 2022/2555 (NIS2) enforcement date approaches, NIS2. a regulation aimed at strengthening cybersecurity across the EU by expanding the scope and increasing the rigor of security requirements, goes into effect on 18 Oct. 2024. Veeam® Software, the #1 market leader by market share in Data Resilience, commissioned a new survey from Censuswide that revealed that only 43% of EMEA IT decision-makers believe NIS2 will significantly enhance EU cybersecurity. This is despite an overwhelming 90% of respondents reporting at least one security incident that the NIS2 directive could have prevented in the past 12 months. Alarmingly, 44% of respondents experienced more than three cyber incidents, with 65% of those categorised as "highly critical".

The survey results, which encompass the views of 500+ IT decision-makers from Belgium, France, Germany, the Netherlands, and the UK, revealed the state of play less than a month before this directive takes effect on Oct. 18. Although nearly 80% of businesses are confident in their ability to eventually comply with NIS2 guidelines, up to two-thirds state they will miss this imminent deadline.

Barriers to NIS2 Compliance

Achieving NIS2 compliance requires businesses to implement essential measures, such as defining incident response plans, securing supply chains, assessing vulnerabilities, and evaluating overall security levels. This includes all affiliated organisations, partners, and supply chains. However, several barriers to compliance persist. Key challenges cited by IT decision-makers include technical debt (24%), lack of leadership understanding (23%), and insufficient budget/investments (21%). Notably, 40% of respondents reported decreased IT



budgets since the political agreement for NIS2 was proclaimed effective in January 2023, despite its stringent penalties, which are comparable to those of the EU's flagship data privacy legislation, the General Data Protection Regulation (GDPR). 63% of respondents view the GDPR as strict, and 62% express the same sentiment about NIS2.

Competitive Pressures Amid Cyberthreats

The slow pace of NIS2 adoption is likely due to the multitude of competing priorities and business pressures that face these organisations. Respondents rank NIS2 lower in urgency than ten other issues, including the skills gap, profitability, and digital transformation. Worryingly, 42% of respondents who consider NIS2 insignificant for EU cybersecurity improvements attribute this to inadequate consequences of noncompliance, which has led to widespread apathy towards the directive.

Additional key findings from the survey include:

• 74% of respondents see NIS2 as

- beneficial, but 57% doubt it will have any substantial impact on overall EU cybersecurity posture.
- Other barriers include a lack of focus on NIS2 compliance (20%), tight timelines (19%), cybersecurity skills shortage (19%), directive complexity (19%), and organisational silos (19%).

Andre Troskie, EMEA Field CISO at Veeam, said: "NIS2 brings responsibility for cybersecurity beyond IT teams into the boardroom. While many businesses recognise the importance of this directive, the struggle to comply found in the survey highlights significant systemic issues. The combined pressures of other business priorities and IT challenges can explain the delays, but this does not lessen the urgency."

"Given the rising frequency and severity of cyberthreats, the potential benefits of NIS2 in preventing critical incidents and bolstering data resilience can't be overstated. Leadership teams must act swiftly to bridge these gaps and ensure compliance, not just for regulatory sake but to genuinely enhance organisational robustness and safeguard critical data," he added.

www.tahawultech.com OCTOBERR 2024



SECURITY FIRST

NED BALTAGI, MANAGING DIRECTOR, MIDDLE EAST, AFRICA, AND TURKEY AT SANS INSTITUTE, TELLS ANITA JOSEPH ALL ABOUT THE OPPORTUNITIES AND CHALLENGES POSED BY AI AND HOW SANS INSTITUTE IS WORKING TO ADDRESS THESE ISSUES.

ybersecurity Awareness
Month is a great
opportunity for
organisations to bolster
their security practices.
How is SANS Institute planning to
address the specific challenges that AI
technologies present to cybersecurity
this October?

Today, AI technologies are essential in detecting and responding to emerging

cyber threats, bringing the potential to enhance cybersecurity by adding a level of automation to threat detection, response, and recovery. Generative AI tools like ChatGPT, Google Gemini, and others are transforming how individuals, teams, and entire organisations operate. They can help drive innovation, offer new avenues to problem-solving, and boost productivity - but as with any new technology, its integration presents

unique challenges and risks.

During Cybersecurity Awareness
Month this October, SANS Institute is
focusing on addressing the emerging
threats posed by AI technologies and
different levels of AI implementation,
with our 2024 Cybersecurity Awareness
Month toolkit. As AI becomes increasingly
integrated into business operations,
it introduces new vulnerabilities
that cybercriminals can exploit. Our

12 OCTOBERR 2024 www.tahawultech.com

engagement with GenAI and ML not only encompasses training and education but also extends to ongoing research, community building, and shaping industry standards, preparing cybersecurity professionals for an AI-integrated future.

As Al technologies become increasingly integral to business operations, what are some of the key risks and vulnerabilities that organizations should be aware of when integrating Al into their systems?

As businesses increasingly integrate Al into their operations, one major risk is over-dependence on Al for critical decision-making, which can lead to complacency. Automated systems, while efficient, are not infallible and lack the human ability to interpret nuances, potentially causing harmful outcomes. Relying too heavily on Al without human oversight can lead to errors, especially in complex situations where Al may misinterpret data or provide biased outcomes.

Another significant risk lies in the security and ethical concerns associated with Al. Al models can inadvertently create new vulnerabilities, such as Al-generated phishing scams or deepfake technologies, which can be exploited by cybercriminals. Additionally, securing AI models and the vast amounts of data they process poses a unique challenge. Al systems often require large datasets for training, which, if compromised, can expose sensitive information. Moreover, attackers can manipulate AI systems to bypass traditional defences, and the opaque nature of some Al decision-making processes complicates accountability.

Ensuring a balance between AI and human intervention is essential

to avoid costly errors or unintended consequences.

SANS aims to help professionals get acquainted with AI and its implications. What are some practical steps or strategies that organisations can implement to securely manage AI technologies and minimise potential risks?

First and foremost, keep in mind that GenAl tools do not possess ethical or moral reasoning and should not replace human judgment. Organisations can better understand and manage the risks associated with Al by prioritising a thorough understanding of the technology and how to regulate its usage, before implementing it.

For example, Generative AI tools operate based on large language models (LLMs) trained on massive datasets, and understanding how these tools work is essential for effective usage. Many LLM-based tools may train their models on any data submitted in prompts and conversations. Private data needs to be kept out of these types of systems.

Whether GenAI is introduced to your organisation from the executive ranks or organically from individual contributors it's important to develop meaningful policy and implementation processes for a safe and effective adoption. Moreover, ensuring that all users receive training in common GenAI risks, prompt engineering and the acceptable use of AI will help manage the risks associated with AI.

How can organisations balance the need for innovation and competitive edge with the necessity of robust security practices when deploying AI tools? Are there any best practices

SANS recommends for maintaining this balance?

Organisations can encourage innovation while ensuring security by maintaining consistency throughout their AI initiatives. At SANS, we recommend starting with a security-first mindset. AI systems should be built with security integrated at every stage, from development to deployment, ensuring vulnerabilities are addressed early. Regular training is another key best practice. Keeping security teams updated on the latest AI advancements and threats through ongoing education ensures they're equipped to handle new challenges.

One such method is prompt engineering, the practice of crafting detailed and precise prompts to guide AI tools to generate accurate and relevant output. Effective prompt engineering helps deliver high-quality output while increasing efficiency and accuracy in AI-assisted tasks. Poorly constructed prompts, on the other hand, can lead to ambiguous and inconsistent results.

As part of an organization's AI strategy, security teams should teach employees how to develop better prompts. By framing clear and specific instructions, teams can better harness AI's capabilities while minimising errors. This is especially important when balancing innovation with security, as clear prompts can help direct AI tools towards desired outcomes while avoiding unintended risks.

Most importantly, ensure that Al systems work alongside qualified security teams. Al can provide valuable insights, but human expertise is necessary for interpreting and acting on these insights. It is imperative to have a human review all Al-generated content to catch errors and biases, manage ethical considerations, maintain transparency, and weigh the pros and cons in complex decision-making. A collaborative culture is important; encourage your teams to question and validate Al-generated outputs, keeping a sharp and critical eye on Al decisions.

OUR ENGAGEMENT WITH GENAI AND ML NOT ONLY ENCOMPASSES TRAINING AND EDUCATION BUT ALSO EXTENDS TO ONGOING RESEARCH, COMMUNITY BUILDING, AND SHAPING INDUSTRY STANDARDS.

www.tahawultech.com OCTOBERR 2024 13

TWO-THIRDS OF HEALTHCARE ORGANISATIONS HIT BY RANSOMWARE: SOPHOS

ophos, a global leader of innovative security solutions for defeating cyberattacks, released a sector survey report. "The State of Ransomware in Healthcare 2024," which revealed that the rate of ransomware attacks against healthcare organisations has reached a four-year high since 2021. Of those organisations surveyed, two-thirds (67%) were impacted by ransomware attacks in the past year, up from 60% in 2023. The rising rate of ransomware attacks against healthcare institutions contrasts with the declining rate of ransomware attacks across sectors: the overall rate of ransomware attacks fell from 66% in 2023 to 59% in 2024.

Alongside an increase in the rate of ransomware attacks, the healthcare sector reported increasingly longer recovery times. Only 22% of ransomware victims fully recovered in a week or less, a considerable drop from the 47% reported in 2023 and 54% in 2022. In addition, 37% took more than a month to recover, up from 28% in 2023, reflecting the increased severity and complexity of attacks.

"While we've seen the rate of

ransomware attacks reach a kind of "homeostasis" or even declining across industries, attacks against healthcare organisations continue to intensify, both in number and scope. The highly sensitive nature of healthcare information and need for accessibility will always place a bullseye on the healthcare industry from cybercriminals. Unfortunately, cybercriminals have learned that few healthcare organisations are prepared to respond to these attacks, demonstrated by increasingly longer recovery times. These attacks can have immense ripple effects, as we've seen this year with major ransomware attacks impacting the healthcare industry and impacting patient care," said John Shier, field CTO, Sophos.

"To combat these determined adversaries, healthcare organisations must adopt a more proactive, humanled approach to threat detection and response, combining advanced technology with continuous monitoring to stay ahead of attackers."

Additional findings from the report include:

 Ransom Recovery Costs Surge: The mean cost of recovery in a healthcare ransomware attack was \$2.57 million in 2024, up from \$2.2 million in 2023 and double the 2021 cost

- Ransom Demands vs Payments: 57% of healthcare institutions that paid the ransom ended up paying more than the original demand
- Root Cause of Attack: Compromised credentials and exploited vulnerabilities were tied for the number one root cause of attack, each accounting for 34% of attacks
- Backups Targeted: 95% of healthcare organisations hit by ransomware in the past year said that cybercriminals attempted to compromise their backups during the attack.
- Increased Pressure: Organisations whose backups were compromised were more than twice as likely to pay the ransom to recover encrypted data [63% vs. 27%]
- Who Pays the Ransom: Insurance providers are heavily involved in ransom payments, contributing in 77% of cases. 19% of total ransom payment funding comes from insurance providers

The latest Sophos report on real-world ransomware experiences explores the full victim journey, from attack rate and root cause to operational impact and business outcomes, of 402 healthcare organisations. The results for this sector survey report are part of a broader, vendor-agnostic survey of 5,000 cybersecurity/IT leaders conducted between January and February 2024 across 14 countries and 15 industry sectors.

ONLY 22% OF RANSOMWARE VICTIMS

→ FULLY RECOVERED IN A WEEK OR LESS, A

CONSIDERABLE DROP FROM THE 47% REPORTED
IN 2023 AND 54% IN 2022.

14 OCTOBERR 2024 www.tahawultech.com



www.tahawultech.com OCTOBERR 2024

MAKING SECURITY VISIBLE

WALID NATOUR, SENIOR MANAGER - SECURITY ENGINEERING, TENABLE, TELLS ANITA JOSEPH WHY EFFECTIVE CYBER EXPOSURE MANAGEMENT IS CRITICAL FOR A ROBUST DEFENCE AGAINST MODERN-DAY ATTACKS.

hat are the main challenges customers face while trying to manage their cybersecurity exposure across different regions like the Middle East, Africa, and Turkey?

Rapid advancements in technology and digital transformation make it challenging for organisations to stay one step ahead of attackers as they try to manage the cybersecurity of their diverse digital assets across a converged IT/OT, IoT landscape that often spans across geographical locations.

Scattered products, isolated views and disjointed teams make it difficult for organisations to hold back threats across the attack surface and identify novel blind spots. Addressing cyber exposure is particularly challenging when it comes to managing the risks of different types of assets on premises and in the cloud. Security gaps caused by misconfigurations, risky entitlements and vulnerabilities have become the epicentre of cyberattacks.

Amidst all that complexity, security leaders need to know if they're exposed and where? Ultimately they need to:

- Know their weaknesses with an all-inclusive view of cyber risk that uncovers the truth about deadly gaps across all assets and attack pathways.
- Expose their risk by identifying, understanding and quantifying the cyber weaknesses with the greatest potential to erode the enterprise's value, reputation and trust.
- Close their gaps by taking swift action



to eradicate priority cyber exposures anywhere to reduce business risk everywhere.

The challenge is gaining the needed holistic visibility to create context around their risk to make the best decisions about remediating vulnerabilities — and removing over-privileged access to cloud resources.

By radically unifying security visibility, insight and action across the entire

attack surface, whatever it is and wherever it exists, modern organisations can protect against attacks from IT to the cloud to OT and everywhere in between.

How can companies in highly regulated sectors like banking and healthcare stay compliant with standards like PCI while still managing their broader cybersecurity risks?

There are a number of standards that

16 OCTOBERR 2024 www.tahawultech.com

organisations operating in highly regulated sectors must remain compliant with. There is PCI DSS 4.0 (Payment Card Industry Data Security Standard) for those that process, store or transmit card data: the CIS (Center for Internet Security) Benchmarks designed to harden systems and applications from attack while maintaining overall system functionality; GDPR (General Data Protection Regulations) that govern how personally identifiable information is used and stored, plus other local mandates including UAE NESA, Qatar 2022 Cybersecurity Framework and Saudi Arabia's National Cybersecurity Authority (NCA) released OTCC. The purpose of all these regulations is to ensure that companies, ultimately, maintain a secure environment.

The reality is that, while adherence with regulatory principles and following frameworks will strengthen defences, alone it does not equate to being secure. Compliance is no substitute for maintaining strong cyber hygiene. The responsibility has to be on every organisation to implement secure working practices that protect their infrastructure and the sensitive data and critical systems contained.

True cybersecurity means knowing your weaknesses, exposing the gaps and then taking steps to close the true exposures that exist within the entire infrastructure. To mitigate the risks across the attack surface, it is essential to gain full visibility — from IT infrastructure to cloud environments to critical infrastructure and everywhere in between - the interdependencies that exist for critical functionality, and determine where weaknesses and vulnerabilities exist. From this position, security teams can then take the necessary steps to remediate the risks where possible, or monitor the assets related to the risk for deviations that could be indicators of attacks.

In your experience, what are the most common vulnerabilities that companies overlook when implementing cloud and container security solutions?

Cloud deployments are arguably the

TRUE CYBERSECURITY MEANS KNOWING YOUR WEAKNESSES, EXPOSING THE GAPS AND THEN TAKING STEPS TO CLOSE THE TRUE EXPOSURES THAT EXIST WITHIN THE ENTIRE INFRASTRUCTURE.

greatest area of risk exposure for organisations. As cloud infrastructure is increasingly central to business operations the threat landscape has evolved, creating substantial points of vulnerability. These include the "toxic cloud triad" of cloud workload risks – those that are:

- publicly exposed;
- critically vulnerable; and
- highly privileged.

In fact, a study from Tenable published earlier this year found that some 95% of cloud security professionals reported cloud related breaches, with 92% reporting that their sensitive data was exposed and 58% of those acknowledged that the sensitive data exposure caused harm.

Among security risks to their cloud infrastructure, respondents ranked insecure human/service identities and permissions, and cloud misconfigurations, at the top (39%). The biggest challenges to securing identities and permissions included lack of visibility (53%) and difficulty in managing entitlements in a multi-cloud environment (50%). Of the organisations that suffered cloud-related breaches, a striking 99% cited identities and permissions risk as the cause.

Effectively securing the cloud requires looking across every aspect of potential exposure including vulnerabilities, configurations and identities

Today, visibility across the entire IT infrastructure is critical in shaping a cybersecurity framework. How does Tenable's Exposure Management platform help businesses achieve complete visibility?

Tenable One is a singular platform built to solve the central challenge of modern

security: a deeply divided approach to seeing and doing battle against cyber risk. It radically unifies security visibility, insight and action across the attack surface, equipping modern organisations to isolate and eradicate priority cyber exposures from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. With Tenable One, enterprises have a single, unified view of risk truth across all types of assets and attack pathways. It connects the dots between the lethal relationships that span solution silos, rapidly finding and fixing the priority exposures that drive up business risk.

- Tenable One's comprehensive inventory provides visibility into the entire external and internal attack surface, identifying unseen and unmanaged assets and risk that could open the door for attackers.
- Tailored exposure views provide security teams with quantified, business-aligned views of what matters most, including highest-risk assets by business function, security domains posing the greatest risk and the security posture of peers.
- Attack path analysis maps critical asset, identity and risk relationships to pinpoint high-risk attack paths before any attack or material impact to the organisation is underway.

Ultimately, Tenable One puts risk in context, enabling organisations to isolate and eradicate the exposures that represent their biggest business threats. Rather than fix every weakness, analysts can focus on choke points with the power to eliminate hundreds of interconnected attack paths. Prescriptive guidance ensures teams can act with maximum speed and confidence.

17

www.tahawultech.com OCTOBERR 2024



TRANSFORMING CYBER DEFENCE

In a rapidly evolving digital landscape, the need for robust cybersecurity measures has never been more critical. As threats become increasingly sophisticated, organisations are turning to innovative solutions to safeguard their assets. SentinelOne's Purple AI stands at the forefront of this revolution, offering a powerful tool that simplifies threat detection and empowers analysts of all skill levels. In a candid chat, Meriam El Ouazzani, Senior Regional Director, Middle East, Turkey and Africa at SentinelOne, speaks to Anita Joseph about Purple AI and how it is transforming new-age security.

hift from Signature-Based Solutions SentinelOne is at the forefront of the AI revolution, taking a huge leap from traditional security approaches. In Meriam's words: "Traditionally, cybersecurity relied heavily on signaturebased solutions, which required known attack signatures to block threats. This method proved limiting, as it could not effectively identify new or unknown attacks. SentinelOne recognised this gap and developed an Al-driven platform that employs advanced algorithms for threat detection. This shift not only enables early identification of threats but also

facilitates a faster response, dramatically improving security outcomes."

Safeguarding Critical Data

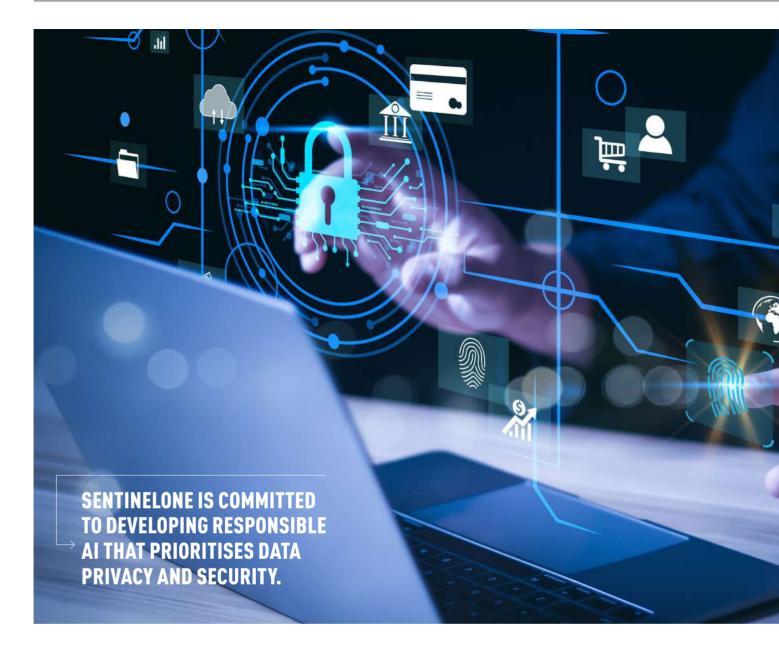
Purple AI is a comprehensive solution designed for data protection and privacy. Meriam says, "Purple AI is never trained with customer data and is architected with the highest level of safeguards. We see a lot of hacks now happening with AI as well, and we have the responsibility to make sure that whatever AI is doing today is real and safe."

A Seamless Experience

Purple Al is a game changer. "One of the standout features of SentinelOne's

THIS INNOVATIVE PLATFORM NOT ONLY
ADDRESSES THE PRESSING CHALLENGES OF THE
CYBERSECURITY SKILLS GAP BUT ALSO ENHANCES
OVERALL OPERATIONAL EFFICIENCY.

www.tahawultech.com OCTOBERR 2024 '



Purple AI is its ability to use natural language for threat hunting," Meriam points out. "This user-friendly approach democratises cybersecurity, allowing analysts—even those with minimal technical expertise—to interact with the platform effectively. By transforming simple queries into complex actions, Purple AI empowers even junior analysts to perform advanced threat analysis, significantly enhancing the efficiency of security operations."

Bridging the Skills Gap

The cybersecurity skills gap is

a huge concern, and Purple AI steps in to address this gap. "The intuitive interface of Purple AI addresses a common concern among organisations: the cybersecurity skills gap. Many companies struggle to find qualified personnel, but SentinelOne's platform allows less experienced staff to participate actively in threat detection. With this approach, organisations can optimise their workforce, reducing the need for a large number of highly specialised analysts while boosting overall productivity," Meriam says.

The Importance of a Unified Platform

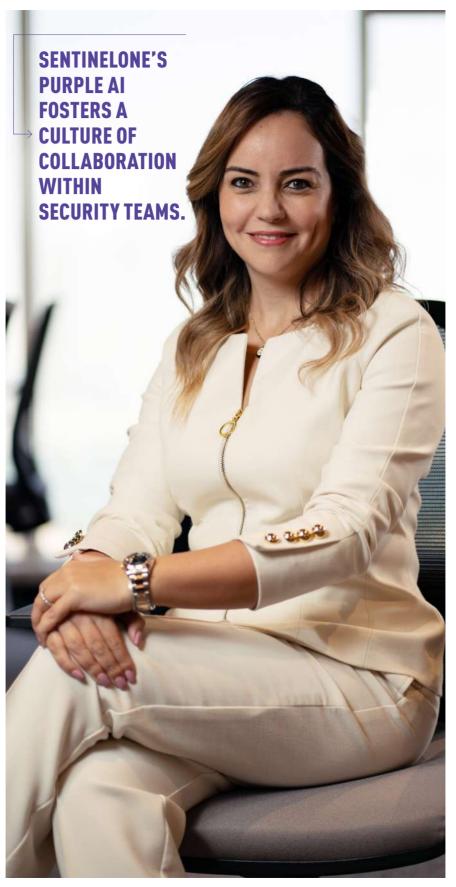
In an era where a unified cybersecurity platform is vital for comprehensive defence against threats, SentinelOne's singularity platform integrates data from multiple sources—both internal and external—offering a holistic view of security operations. "This cohesive framework reduces complexity and enables real-time analysis, allowing analysts to take informed actions swiftly. By centralising data, the platform enhances collaboration among teams, ensuring that security measures are both effective and efficient," adds Meriam.

20 OCTOBERR 2024 www.tahawultech.com



Looking Ahead: The Future of Al in Cybersecurity

The evolution of AI in cybersecurity is just beginning. "SentinelOne is committed to developing responsible AI that prioritises data privacy and security. The ongoing research and development efforts aim to enhance the capabilities of Purple AI, enabling organisations to stay one step ahead of emerging threats. As the landscape continues to change, the integration of AI in cybersecurity will play a pivotal role in shaping the future of threat detection and management," Meriam says.



www.tahawultech.com OCTOBERR 2024



PURPLE AI IS NEVER TRAINED WITH CUSTOMER

→ DATA AND IS ARCHITECTED WITH THE HIGHEST LEVEL OF SAFEGUARDS.

A New Era of Collaboration and Learning

SentinelOne's Purple AI fosters a culture of collaboration within security teams. Analysts can share queries and findings, promoting collective learning and improving overall threat response. Even team members without a technical background can engage in threat hunting exercises, demonstrating the platform's accessibility and potential to develop a more skilled workforce.

Empowering the Next Generation of Cybersecurity

SentinelOne's Purple AI represents a significant leap forward in cybersecurity technology. By simplifying complex processes and enabling a broader range of users to engage in threat detection, it transforms the landscape of cybersecurity. As organisations continue to navigate the challenges of the digital age, tools like Purple AI will be essential in empowering teams to protect against ever-evolving threats. In this new era, cybersecurity is no longer the sole domain of experts; it is a collective effort, open to all.

SentinelOne's Purple Al represents a paradigm shift in how organisations approach cybersecurity. By making advanced threat detection accessible to a broader range of users, it empowers teams to work collaboratively in the face of evolving threats. This innovative platform not only addresses the pressing challenges of the cybersecurity skills gap but also enhances overall operational efficiency. As businesses continue to navigate an increasingly complex digital landscape, tools like Purple Al will be essential in equipping them to protect their assets and data. In this new era of cybersecurity, the focus is not just on advanced technology, but on empowering people—making cybersecurity a collective effort that is inclusive, effective, and resilient. 1

OCTOBERR 2024 www.tahawultech.com



Hosted b

غــرفــة ديـــي CHAMBER اABUC لا قملة DIGITAL 13 - 16 OCT 2024 DUBAI HARBOUR

FEATURING



FUTURE BLOCKCHAIN SUMMIT Fintech SURGE.

Marketing Mania

THE WORLD'S LARGEST STARTUP & INVESTOR EVENT

DREAM BIG. SCALE BIGGER!

UNITING FOUNDERS, INVESTORS & CORPORATE INNOVATORS TO CO-CREATE OUR FUTURE

1,800⁺ STARTUPS

100 COUNTRIES **70,000** VISITORS

1,200 INVESTORS

450⁺
SPEAKERS



WWW.EXPANDNORTHSTAR.COM

in f (





#EXPANDNORTHSTAR

Inspired by





بريادا والكال براء الأمار DUBAI WORLD TRADE CENTRE



tahawultech.com

CISO50 & FUTURE SECURITY AWARDS 2024

CELEBRATING EXCELLENCE

he CISO 50 and FSA
Awards celebrate not just
achievements, but resilience,
innovation and the unwavering
commitment to cybersecurity in an
increasingly complex digital landscape.

Today, it's become impossible to ignore the profound impact that artificial intelligence is having on our industry. Al is transforming how we approach cybersecurity, offering powerful tools for threat detection, incident response, and data analysis. However, with these advancements come significant challenges. Cybercriminals are harnessing Al just as effectively, deploying sophisticated attacks that

can outpace traditional defenses. This dual-edged sword presents a tightrope for today's Chief Information Security Officers.

In this context, the leadership qualities we celebrate through the awards—vision, adaptability, and courage—are more crucial than ever. The award winners here have not only embraced the challenges posed by AI but have also turned them into opportunities. They exemplify what it means to be a leader in cybersecurity today.

These outstanding individuals and organisations have developed innovative strategies and solutions that enhance security while enabling growth and efficiency. They've implemented

frameworks that not only protect their own organisations but also serve as models for others in the industry. Their work inspires us all to strive for excellence and to push the boundaries of what's possible in cybersecurity.

As we recognise the winners of the CISO 50 and FSA Awards tonight, let us reflect on their achievements. They represent the forefront of our battle against cyber threats, and their commitment to security empowers us all to face the future with confidence. They remind us that cybersecurity is not just a technical challenge; it is a vital component of our business strategy and a key driver of trust in the digital age.









www.tahawultech.com OCTOBER 2024 2



tahawultech.com CISO50 AWARDS 2024



Mohamed Riyasudeen
Al Ain Ahlia Insurance Company
(PSC)



Hussain AlKhalsan Zand Bank



Dhiraj Sasidharan



Kapil Matta Agthia Group PJSC



Waqas Haider
HBL Microfinance Bank



Mohammed Azam EMSTEEL

www.tahawultech.com OCTOBER 2024 27



Ali Othman
HSBC Bank Middle East Limited



Chenthil Kumar
Red Sea International (RSI)



Rizwan Ahmed
Emirates Investment Bank



Zaheer Mubarak Shaikh Al Maryah Community Bank LLC (Mbank)



Sajin Shivdas
Family Development Foundation



Irshad SyedGAC Group



Anoop Kumar Paudval
Gulf News, Al Nisr Publishing LLC



Eng. Abdulwahab Al Gamhi
Federal Authority for Identity, Citizenship,
Customs & Port Security - UAE



Abdulla Alhashmi 7X



Shafiullah Ismail Mubadala Capital



Kiran Kumar Alpheya Group



Santosh Pathak
King's College Hospital London, Dubai

29

www.tahawultech.com OCTOBER 2024



Jayesh Nandanan Mediclinic Middle East



Mohammad Wail Khachfa
Department of Digital Ajman,
Government of Ajman



Kashif Khan
Abu Dhabi National Insurance Company
PJSC (ADNIC)



Dr. Lt. Col. Hamad Khalifa Al NuaimiAbu Dhabi Police General Headquarters



Abdulla Albreiki
Al Yah Satellite Communications
Company P.J.S.C. (Yahsat)



Nagarajan Manivannan Mashreq



Ankit Satsangi BEEAH Group



Rejish Krishnan Kandath Network International



Ibrahim Adedeji Adefila Al Rostamani Group



Taaleem



Appas Muthalif
DP World



Nisha Rani MMI - Emirates Leisure Retail

31

www.tahawultech.com OCTOBER 2024



Toufeeq Ahmed
Gargash Group



Abhinav Kumar Shrivastava NMC Healthcare



Rohit Anand Bajpai
Gulf Islamic Investments LLC



Will Douglas
Premier Inn



tahawultech.com CISO50 AWARDS 2024



Jordan Savvides
Global CISO Advisory



Talal Ibrahim Albalas Abu Dhabi Quality and Conformity Council,

Government of Abu Dhabi

Prabhat Pathak Gulf Marketing Group (GMG)

Dr. Ahmed Alketbi Dubai Electricity & Water Authority (DEWA)

Khaled Altenaiji Emirates National Oil Company Group (ENOC)

Ahmad Al Shami Juma Al Majid Holding Group LLC

Asif Patankar STORY Hospitality

Lt. Col. Saeed AlShebli Ministry of Interior - UAE

Kausar Mukeri GEMS Education

Amal Bader Albusaeedi Emirates Red Crescent (ERC)

Arif Irfani Sharjah Islamic Bank (SIB)

Sunil Nair Majid Al Futtaim Retail

Manoharan Mudaliar Truebell Group of Companies

Sagar Sethi First Abu Dhabi Bank (FAB)

Mukesh Kumar Apparel Group

Muhammad Irfan Ali CAFU

www.tahawultech.com OCTOBER 2024 3



FUTURE SECURITY AWARDS 2024



CybleBest Product for MSSPs of the Year



VEEAMBest Data Protection Vendor of the Year



Commvault
Best Cyber Resilience Leader of the Year



StarLinkBest Security Value Added Distributor of the Year

www.tahawultech.com OCTOBER 2024



Best Data Analytics Vendor of the Year



Sophos
Best Cybersecurity System
Vendor of the Year



Best Managed Detection and Response Service Provider of the Year



Vectra Al

Best Artificial Intelligence Cybersecurity
Vendor of the Year



Help AG

Best Managed Security Services
Provider of the Year



Cloud Box Technologies

Best Digitalisation & Cybersecurity
Provider of the Year



Juniper Networks
Best Cloud Networking Vendor of the Year



EVADBest Emerging Cybersecurity
Distributor of the Year



Almoayyed Computers Middle East (ACME)

Best Cybersecurity Solutions Provider of the Year



Cloudflare
Best Cloud Security Vendor of the Year



Ring

Best Smart Home Security System of the Year



ManageEngine

37

Best Identity and Access Management Vendor of the Year

www.tahawultech.com OCTOBER 2024



LinkShadowBest Security Vendor of the Year



FUTURE SECURITY AWARDS 2024



SANS Institute

Most Innovative Cybersecurity Training Programs of the Year

Hikvision

Best Artificial Intelligence Security Vendor of the Year

OPSWAT

Best Critical Infrastructure Security Vendor of the Year

Mindware

Innovative AI Distributor of the Year

AQUILA PRO AI by D-Link

Best Al Innovative Product of the Year



Bye-bye blind spots.

Pan-Tilt Indoor Camera

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

To learn more, visit us at **GITEX Global 2024** Stand H20-B05



ring an **amazon** company



360° Pan & 169° Tilt Coverage



Live View & Two-Way Talk



Manual Audio & Video Privacy Cover



HD Video & Colour Night Vision



Plug-In Power



Pets Camera













ML VERSUS HACKERS: HOW BEHAVIORAL ANALYTICS ARE CHANGING THE RULES OF THE GAME

ALEXEY POTAPOV. ATTACK DETECTION DEPARTMENT EXPERT, PT EXPERT SECURITY CENTER. POSITIVE TECHNOLOGIES



ecurity information and event management or SIEM can detect attacks in different ways including building chains of launched processes based on normalised events. automated whitelisting, and machine learning (ML) to detect suspicious user behavior and infrastructure processes. The Behavioral Anomaly Detection (BAD) module is nothing new. It works as a second opinion system, collecting data about events and users, assigning them a risk score, and generating an alternative opinion based on its algorithms. BAD reduces the cognitive load on SIEM system analysts so they can make more informed decisions about information security incidents.

In this article, we'll discuss what elevates BAD from "just another tool" to an indespensible force on your cybersecurity team capable of doing things you never could before.

Event risk scoring in BAD

At the heart of the BAD module is how it scores event risks to ensure the early detection of potential threats using ML algorithms. Each event is assigned a risk score based on an analysis and comparison of behavioral patterns against normal activity.

At the center of the module and the most important thing BAD does is operating system process analysis. Risk scoring is based on the idea that the root cause of most cyberthreats in internal infrastructure is operating system processes. They are how attackers actually carry out their plans.

The way BAD scores risks is different

than in user and entity behavior analytics (UEBA) systems and other similar solutions. Risk scoring in the BAD module begins when it receives events from operating systems and applications, each of which it analyzes using a variety of atomic machine learning models designed to study different aspects of the same events and processes. This approach ensures that all scores reflect a multifaceted assessment.

Atomic models are particularly interesting because they analyse individual features of events, allowing the same event to be assessed from different angles. For example, one model might focus on identifying rare or unique processes, while another looks at communication with network resources. Thanks to BAD's native ability to search and combine different types of events (for example, to create a data set that looks for an anomalous process logging into the operating system or application). we were able to use the verdicts of such models in BAD's general process profiler. Without combining such events in the same data set, we wouldn't be able to use models that analyse operating system and application access.

AT THE HEART OF THE BAD MODULE IS HOW IT ightarrow scores event risks to ensure the early DETECTION OF POTENTIAL THREATS USING ML ALGORITHMS.

Each atomic model has a certain weight (significance) to calibrate the final risk score more accurately. Model triggers are aggregated for each globally unique identifier (GUID) taking into account process launch event models and the numerous other events in which the process participates. This provides a diverse context of the process' interactions with the system, including all associated process sequences in the chain.

Indicators of behavior

BAD moves beyond traditional threat detection methods that rely on specific attacker tools or artifacts (attack indicators, IP addresses, hashes). Attacker indicators of behavior (IoB) are a key element in this process, as they comprise long-term rules that are difficult to bypass and provide important information for analysis when triggered.

BAD includes a group of specialised IoB rules that are activated when certain conditions are met during process analysis. These indicators are triggered when anomalous or suspicious activity is detected in a process' GUID based on behavioral models.

Indicators of behavior have one main job: expose the strategy and goals of attackers by analyzing sequences of actions that form malicious patterns and stand out compared to ordinary behavior on the network. IoB serve as a signal that investigation is needed and lead to the generation of alerts sent automatically to MaxPatrol SIEM, our central security information and event management system. The final risk score for each process and its chain is formed by aggregating the weight scores of the models triggered when detecting indicators of behavior. This risk score can be used to prioritise events so SIEM system analysts can focus only on the most critical and suspicious events. Indicators of behavior can also be used to make advanced correlation or enrichment rules that provide more accurate and comprehensive threat detection.

Figures 1 and 2 show how the process profile and its risk score are formed.



Figure 1. How a process profile is formed

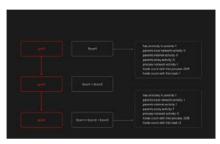


Figure 2. How a process risk score is formed

From theory to practice: detecting cyberattacks with BAD

Almost all alerts generated in the SIEM system are sent to the BAD module to enrich them with the same risk score requested through the event card snippet (Fig. 3). This allows MaxPatrol SIEM analysts and operators to use the bad. risk_score field when writing correlation or enrichment rules, as well as in the event filter (for example, to sort and search for the most anomalous triggers).

BAD can detect the following cases:

- Complex targeted attacks and attacks that bypass correlation rules.
- New tactics, techniques, and procedures not yet covered by detection rules.
- Post-exploitation after the exploitation of a previously unknown vulnerability.
- Accidental or excessive whitelisting (when users themselves whitelist certain correlation rules).

Case 1. BAD for second opinions and ranking triggered correlation rules using bad.risk_score One great thing about BAD is that it helps analysts evaluate correlation rule triggers. The risk score in the triggered correlation rule's event card can be the deciding factor in confirming a true positive or false positive. Figure 3 shows an example of a triggered correlation rule with importance = high. However, BAD analysed the activity of the process that triggered the rule and assigned the event a low risk score. This correlation likely has a low significance level, and the positive is actually a false positive.

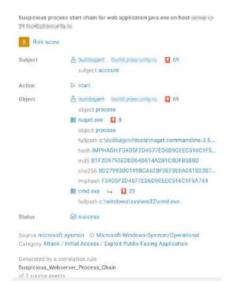


Figure 3. Correlated event card with a risk score from BAD



Figure 4. Triggers of ML models and indicators of behavior

www.tahawultech.com OCTOBERR 2024

Now let's check out which alerts with an enriched bad.risk_score were sent to MaxPatrol SIEM preceding interactive attacks (Fig. 5), and which triggers have a risk score above 50 and 100 (Fig. 6 and 7).

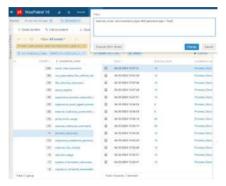


Figure 5. List of triggered correlation rules with an enriched risk score from BAD



Figure 6. Search for correlation rules with risk scores above 50



Figure 7. Search for correlation rules with risk scores above 100

Figures 6 and 7 show that in MaxPatrol SIEM, after filtering the positives by bad.risk_score, only a small number of triggers with a score over 50 remain and no triggers over 100.

Now let's look at two real interactive attacks from the Standoff cyberexercise. We'll start with triggered models and

indicators of behavior in the BAD module in MaxPatrol SIEM and explain how we discovered these incidents.

Case 2. BAD as a second opinion system

Let's consider an incident where the malicious gostbypass.exe file is launched on a user's workstation. The file functions as a SOCKS proxy and is used to develop the attack further, but the malware itself doesn't generate any processes. The attackers conduct reconnaissance of the domain network and gain access to several servers and applications. The chain of events is shown in Figure 8.

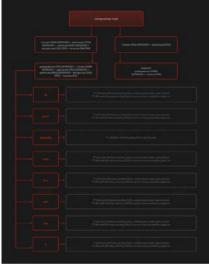


Figure 8. gostbypass.exe activity

Several correlation rules were triggered with a low level of importance (Fig. 9), but the BAD module had an alternative opinion after analysing the behavior profile of the gostbypass.exe process as whole. Operators can check the risk score card and confirm BAD's score (Fig. 10), and the activity will not be part of the subsequent training of models. Figure 11 shows which ML models and indicators of behavior were triggered.





Figure 9. Correlation between high risk scores and the "info" importance level





Figure 11. Triggers of ML models and IoB in the snippet from BAD

DS_Anomaly_Process_Target_Host_and_Port

The BAD module used its machine learning algorithms to analyse the data flow from the compromised

user's workstation. During analysis, the module identified unusual patterns in the sequences and behavior of processes (Fig. 12) based on an integrated group of atomic models and indicators of behavior. Deviations from the baseline profile of normal behavior according to these models influenced the increase in risk score, which signaled the system about potential malicious activity.

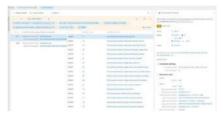


Figure 12. Indicators of behavior sent by BAD to MaxPatrol SIEM

Case 3. BAD as a second opinion and ranking system for triggered correlation rules using bad.risk_score

The third case is an incident where a user's computer was attacked using a malicious office file. The PowerShell script launched from this document downloaded and activated a number of malicious components, one of which served as a proxy server and channel to further compromise the system. The attacker carried out reconnaissance of the node and moved laterally inside the perimeter to gain access to several computers on the network. Figure 13 shows the event diagram.



Figure 13. ss.exe activity

Let's look at the correlation rules in this case with a high bad.risk_score value. In Figure 14, we filtered out all the high-risk triggers (according to BAD).

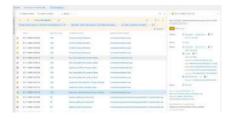


Figure 14. Correlation rules with a high risk score triggered

This illegitimate activity also triggered several correlation rules and indicators of behavior (Fig. 15).



Figure 15. Correlated event card with a risk score from BAD

So which machine learning models were triggered and why did this activity have a high risk score? Figure 16 shows a list of triggered models, and I'll explain a few of them.

 Suspicious chain of process launches (Windows).

MaxPatrol SIEM can build chains of launched processes. We have a pretrained model that was trained and continues to be trained on process chains.

2. Atypical target node for the

process (Windows).

This model looks for anomalous processes authorising in the Windows operating system. If the activity is anomalous, the model will be triggered.

3. Atypical process for users [Windows].

This model looks for processes unique to users launched on a node and warns that the process was not used in training.

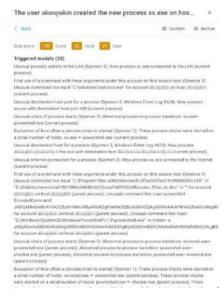


Figure 16. List of models triggered from ss.exe activity

Indicators of behavior were formed based on the triggered atomic models (Fig. 17) and used to generate the final risk score.

Triggered rules (10)

OS_Anomaly_Process_Chain_and_Port
OS_Anomaly_Process_Chain_and_Internet_Activity
OS_Anomaly_Process_Chain_and_Local_Net_Activity
OS_Anomaly_Process_Chain_and_Process_Target_Host
OS_Anomaly_Process_Chain_and_User_Cmdline
OS_Anomaly_Process_Target_Host_and_Port
OS_Anomaly_Process_Target_Host_and_Internet_Activity
OS_Anomaly_Process_Target_Host_and_Local_Net_Activity
OS_Anomaly_Process_Target_Host_and_User_Cmdline
OS_Process_Chain_Frequency_Analyzer_WL

Figure 17. Indicators of behavior triggered

The BAD module identifies the features of processes. Figure 18 shows a detected feature: this illegitimate activity contains a process that behaves like a proxy server.

www.tahawultech.com OCTOBERR 2024

- Abnormal parent process activity: 0 Parent process activity in the LAN: 0
- Parent process activity on the internet: 1
- Parent process anomalies associated with unusual proxy connections: 1 Process activity on the network: 1
- Number of hosts on which a process with this name was started: 1

 Number of hosts on which a process with this hash value was started: 1

 Figure 18. A list of features

Ultimately, BAD identified this anomalous activity, most notably the non-standard use of a process acting as a proxy server. Filtering the correlation rule triggers by bad.risk_score also made it possible to find the necessary triggers fast and detect the incident quickly.

Case 4. BAD as a tool to spot attacks not detected by traditional monitoring tools and operator errors due to excessive whitelisting

Imagine that none of the correlation rules in the system were triggered for the previous activity, or an inexperienced operator wrote a broad regulation and whitelisted a bunch of correlation rules.

Built on alternative detection methods, BAD sends the triggered indicators of behavior to MaxPatrol SIEM, where we aggregate all the triggers in a process GUID and calculate the total weight of all rules. Then we find the most anomalous processes, which are the exact processes that were so important in the previous case. The analysed activity also includes many different types of events throughout the entire chain of processes.



Figure 19. The most anomalous processes in MaxPatrol SIEM

Integration with the MaxPatrol 02 metaproduct

Integration of the BAD module with MaxPatrol O2 (Fig. 20), which builds attack chains automatically, is a perfect complement to the metaproduct's threat detection methods.

Synergy is attained two ways:

- 1.BAD creates its own alerts to help not miss attacks that aren't detected by traditional monitoring tools.
- 2. MaxPatrol 02 joins alerts from BAD into a single attack context formed by the metaproduct using linking and enrichment algorithms. This helps move from analysing atomic alerts to analysing the attack chain. Alerts from BAD are also taken into account. We describe this process in more detail here.

The more complete the attack context, the more accurate MaxPatrol O2's verdict is about the activity. It's obvious that it's easier to make a decision about a suspicious connection to an external node when you can see the entire chain of events that led to the connection and what immediately followed. For example, the creation of files, user authorisations in the system, lateral movement, and much more. Fuller attack context also makes it possible to localise the incident by finding the starting point and responding in a way that makes it impossible for the attacker to continue the attack.

When BAD and MaxPatrol O2 work together, attack detection accuracy improves. Events are analysed in BAD and its verdicts scored in the metaproduct's scoring model. This reduces the number of false positive chain verdicts as in Case 1, where correlations with importance = high were scored as low risk by the BAD module.

RISK SCORING IS
BASED ON THE IDEA
THAT THE ROOT
CAUSE OF MOST
CYBERTHREATS
IN INTERNAL
INFRASTRUCTURE IS
OPERATING SYSTEM
PROCESSES.



Figure 20. BAD integration with MaxPatrol 02

Future plans

It's no secret that machine learning is quickly becoming a powerful tool in detecting attacks. In SIEM systems, ML algorithms help analysts investigate incidents and speed up the detection of anomalies and attacks that may go unnoticed by traditional detection methods based on indicators of compromise (IoC) or indicators of attack (IoA).

Risk scores in BAD improve threat response accuracy and speed, help SOC teams optimize detection processes, and most importantly, reduce the time required to neutralise incidents.

In the future, we plan to improve scoring and integrate BAD with our other products.

We'll also improve atomic models and develop new indicators of attacker behavior to more accurately identify anomalies and characteristic signs of hacker activity.

We also see tremendous potential in creating a single, comprehensive model that describes hacker behavior as a whole. It will be trained on a wide dataset including real cyberincidents from our customers and insights from cyberexercises and projects, including Standoff. Positive Technologies has unique resources at its disposal to collect this data, allowing us to constantly improve and retrain our model.

Combining multiple atomic models and behavior indicators in a largescale analytical solution will open a new world of proactive protection against cyberattacks. Also investments in machine learning and artificial intelligence will propel cybersecurity to new heights and provide our customers with the best protection in a constantly changing digital world.

OPSWAT.

Protecting the World's Critical Infrastructure

Cyberthreat Prevention from Endpoint to Cloud

OPSWAT solutions are trusted by more than 1,500 organizations, governments, and institutions around the world to protect their critical networks. Our platform solves a wide spectrum of specific customer challenges across critical infrastructure.

- Email Security
- Application and File Security
- Storage Security
- Peripheral MediaProtection
- Supply Chain Security
- Cross Domain Security

- OT Security
- Access and Endpoint Security
- Secure Managed
 Transfer
- Malware Analysis and Threat Intelligence
- 0EM

For more information visit: www.opswat.com or contact sales-inquiry@opswat.com







LINKSHADOW REINVENTING CYBERSECURITY



s businesses increasingly depend on digital infrastructure, robust cybersecurity has become essential. The rise of interconnected systems and the vast amounts of data generated from cloud services and on-premises environments heighten the risk of network breaches. Cybercriminals constantly seek vulnerabilities to exploit, leading to significant financial and reputational damage. To combat these threats, organizations must implement solutions that offer real-time monitoring and comprehensive visibility across their

entire network. By effectively detecting anomalies, these measures help safeguard sensitive data and ensure compliance with regulatory standards, ultimately maintaining a strong security posture in today's evolving threat landscape.

Organizations now face the daunting task of managing vast amounts of sensitive information while ensuring security. With cyber threats becoming more sophisticated and frequent, the risk of data breaches, ransomware attacks, and insider threats looms large. Additionally, compliance with a growing number of regulations, such

as regional and global Personal Data Protection Law (PDPL), GDPR, and HIPAA, adds another layer of complexity. Organizations must not only protect their data but also demonstrate adherence to these regulations, which can vary across jurisdictions.

Furthermore, the sheer volume and diversity of data mean that traditional security solutions often struggle to provide adequate visibility and context. Silos between different security tools can hinder effective threat detection and response, leaving organizations vulnerable to potential attacks. This fragmented approach can also lead to

inefficiencies, where security teams spend valuable time trying to correlate data from multiple sources instead of focusing on proactive defense strategies.

As organizations navigate this increasingly complex digital landscape. they face significant challenges in maintaining effective cybersecurity. The rapid growth of remote work and interconnected devices has expanded the attack surface, making it more difficult to monitor and secure network activities. Data breaches have become increasingly common, with thousands of reported incidents in recent years highlighting a troubling trend—there has been a marked increase of around 68% in breaches year over year. The consequences can be devastating; about 60% of small businesses close shortly after experiencing a breach.

Human error plays a significant role in these incidents, contributing to approximately 82% of breaches, often due to issues like stolen credentials. As cyber threats continue to evolve, the

LINKSHADOW'S COMMITMENT TO CYBERSECURITY IS UNWAVERING, CONTINUOUSLY INNOVATING TO PROTECT YOUR DIGITAL LANDSCAPE WITH AIPOWERED SOLUTIONS.

rise of ransomware attacks has become particularly alarming, with predictions indicating that these attacks will occur every 11 seconds. Additionally, regulatory requirements are becoming more stringent, putting further pressure on organizations to ensure compliance.

In this environment, the need for comprehensive cybersecurity measures that enhance visibility and provide realtime insights into network behaviors and anomalies has never been more urgent. Without a proactive approach to monitoring and threat detection, organizations risk falling victim to breaches that can compromise sensitive data and disrupt operations.

These trends highlight the critical

importance of adopting robust solutions to protect sensitive information and mitigate risks in today's complex digital landscape. By embracing innovative technologies and frameworks that integrate seamlessly into their existing infrastructure, organizations can build a resilient security posture that not only defends against current threats but also adapts to the challenges of the future. Investing in advanced monitoring tools and analytics will empower security teams to respond swiftly to incidents, ultimately safeguarding both their data and their reputation in an increasingly volatile environment.

Understanding the Cybersecurity Mesh Architecture Concept

Cybersecurity Mesh Architecture (CSMA) is an innovative approach to designing and implementing cybersecurity measures in a highly interconnected digital landscape. It emphasizes a decentralized and flexible framework that allows organizations to create a security perimeter around their digital assets, regardless of where those assets are located—on-premises, in the cloud, or at remote locations.

At its core, CSMA promotes the idea of a "mesh" of security solutions that work collaboratively rather than relying on a single, monolithic system. This architecture enables organizations to integrate various security tools and technologies, facilitating seamless communication and data sharing among them. By breaking down silos, CSMA enhances visibility across the entire security landscape, allowing for more effective threat detection and response.

One of the key benefits of this architecture is its ability to adapt to



www.tahawultech.com OCTOBER 2024 49

the evolving nature of cyber threats. As organizations increasingly embrace cloud computing and remote work, the traditional perimeter-based security model becomes inadequate. CSMA shifts the focus from a fixed perimeter to a dynamic, flexible approach that adjusts to the needs of the organization.

Moreover, CSMA supports the implementation of Zero Trust principles, which advocate for continuous verification of users and devices, regardless of their location. This enhances security by ensuring that only authenticated and authorized entities can access critical resources.

Enabling LinkShadow NDR in the Mesh

Network Detection and Response (NDR) is a crucial component of Cybersecurity Mesh Architecture, enhancing its effectiveness in real-time threat detection and response. LinkShadow NDR focuses on monitoring network traffic to identify suspicious activities and anomalies, leveraging advanced analytics and machine learning to detect potential threats as they emerge. By continuously analyzing the network, LinkShadow NDR provides organizations with deep visibility into their environments, enabling them to identify patterns indicative of cyberattacks.

In the context of CSMA, LinkShadow NDR complements other security measures by offering a layer of network-centric insights that can inform decision-making across the security mesh. This integration allows for faster identification of threats, improving incident response times and reducing the risk of breaches. As cyber threats become increasingly sophisticated, the ability to detect anomalies in real-time is essential for



organizations to maintain a proactive security posture.

By embedding LinkShadow NDR within a cybersecurity mesh framework, organizations can ensure a more resilient defense, capable of adapting to evolving threats while maintaining comprehensive visibility across their digital assets. This synergy not only enhances overall security effectiveness but also supports the implementation of Zero Trust principles, ensuring that all network activities are scrutinized and validated continuously.

Al-Powered Threat Detection

Al-driven threat detection is essential in the context of Cybersecurity Mesh Architecture (CSMA), particularly when integrated with LinkShadow NDR. By utilizing advanced algorithms and machine learning, Al enhances the capability of LinkShadow NDR to analyze large volumes of network traffic in real time. This allows for the rapid identification of

suspicious activities and anomalies that may indicate a potential threat.

Within the CSMA framework, Al-driven insights help prioritize alerts based on context and severity, reducing false positives and enabling security teams to focus on the most critical incidents. The integration of AI with NDR not only improves the speed and accuracy of threat detection but also facilitates continuous learning from new attack vectors. As the landscape of cyber threats evolves, this synergy ensures that organizations can swiftly adapt their defenses, maintaining a robust security posture across their interconnected digital assets. Ultimately, AI-powered threat detection within CSMA, supported by LinkShadow NDR, empowers organizations to proactively combat emerging threats while enhancing their overall resilience

Strengthening Cybersecurity with UEBA Integration

User and Entity Behavior Analytics (UEBA) is increasingly vital in modern cybersecurity, especially when integrated with NDR and a Cybersecurity Mesh Architecture (CSMA). This powerful combination enhances threat detection and response capabilities across an organization's digital landscape.

STAY AHEAD OF CYBER THREATS WITH OUR NETWORK DETECTION AND RESPONSE SOLUTION,

PROVIDING REAL-TIME INSIGHTS AND PROACTIVE PROTECTION FOR YOUR NETWORK.

LinkShadow UEBA analyzes user and entity behaviors to establish a baseline of normal activity, enabling the identification of anomalies that may indicate potential threats. When paired with NDR, which continuously monitors network traffic for suspicious activities, organizations gain a comprehensive view of their security posture. The CSMA framework further enhances this integration by providing a flexible, interconnected approach to cybersecurity.

Maximizing Security: Open XDR with NDR and CSMA

When combined with LinkShadow's Network Detection and Response (NDR), the benefits are substantial. LinkShadow NDR continuously monitors network activities for anomalies, providing real-time insights into potential threats. By leveraging Open XDR, these insights are enriched with data from other security tools, enabling more accurate threat detection and streamlined incident response.

This synergy allows organizations to respond swiftly to emerging threats, reduce response times, and improve overall security effectiveness. By implementing Open XDR alongside LinkShadow NDR, businesses can

enhance their defense strategies, ensuring robust protection for their critical assets

Data Compliance and Governance

The need for data compliance and governance has become increasingly critical as organizations navigate a complex regulatory landscape and manage vast amounts of sensitive information. Data compliance involves adhering to various laws and regulations, such as regional and global Personal Data Protection Law (PDPL), GDPR, HIPAA, and PCI, which are designed to protect personal data and ensure individuals' privacy rights. Failure to comply with these regulations can result in severe penalties, legal liabilities, and reputational damage.

Introducing LinkShadow DSPM

From its origins in network security, LinkShadow has evolved into Data Security Posture Management (DSPM) with its revolutionary solution designed to ensure not only network security but also comprehensive data security and compliance. This initiative focuses on empowering organizations to strengthen their overall security posture while ensuring adherence to local and

international data protection laws.

The key features of LinkShadow's DSPM include automated data discovery. risk assessment, and real-time monitoring, all of which are essential for organizations seeking to navigate the complexities of data management. Automated data discovery techniques allow businesses to identify and classify sensitive information across various environments—whether onpremises, in the cloud, or within hybrid infrastructures. This capability provides organizations with a clear understanding of their data landscape, enabling them to make informed decisions about data protection strategies.

In addition to discovery, LinkShadow's DSPM integrates sophisticated risk assessment tools that thoroughly evaluate the security posture of data assets. These tools assess compliance with industry regulations and internal policies, helping organizations adhere to best practices while mitigating the risks of potential fines or breaches. By continuously evaluating security measures, organizations can proactively address vulnerabilities and ensure their data is adequately protected.

Real-time monitoring features offer ongoing insights into data access and

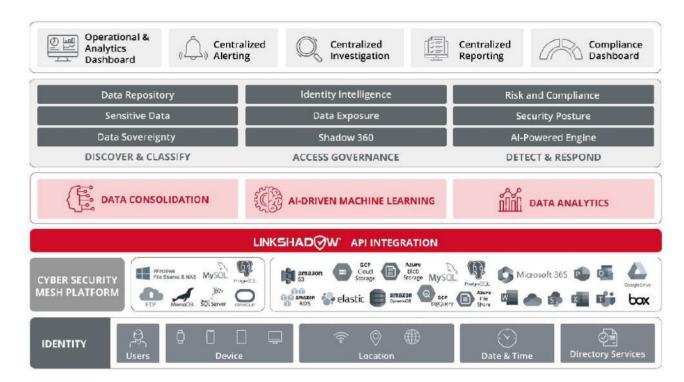
FROM NETWORK
SECURITY,
LINKSHADOW

HAS NOW
EVOLVED INTO
DATA SECURITY
POSTURE
MANAGEMENT.



Data Exposure

www.tahawultech.com OCTOBER 2024 51



usage patterns, enabling organizations to swiftly detect suspicious activities or anomalies. With automated alerts and incident response capabilities, teams can act quickly to mitigate potential threats before they escalate, significantly reducing the likelihood of data breaches.

Moreover, LinkShadow's DSPM provides comprehensive reporting and analytics, allowing security teams to track their data security efforts effectively. This centralized management not only streamlines operations but also fosters a culture of proactive risk management. By equipping organizations with detailed reports, stakeholders can gain visibility into compliance status and

the effectiveness of security measures.

LinkShadow DSPM is designed to offer comprehensive support—from assessing current security measures to implementing tailored strategies that protect sensitive information. By prioritizing data governance and risk management, LinkShadow empowers organizations to manage their cybersecurity more effectively, respond to emerging threats with greater agility, and maintain a strong compliance posture.

In a landscape where cyber threats are constantly evolving, LinkShadow's DSPM equips organizations with the necessary tools to safeguard their data assets. By ensuring resilience against evolving cyber

LINKSHADOW IS COMMITTED TO EMPOWERING PARTNERS WITH INNOVATIVE SOLUTIONS AND SUPPORT.

threats while maintaining regulatory compliance, businesses can protect their reputation and build trust with customers and stakeholders. This holistic approach not only enhances security measures but also positions organizations to thrive in an increasingly digital world.

Empowering Channel Partners

LinkShadow recognizes that collaboration is key to successful cybersecurity, particularly in a landscape where threats are constantly evolving. To this end, the company has developed an extensive channel partner program designed to equip partners with the training, resources, and support they need to deliver exceptional value to their clients.

By enabling partners to leverage the





Cybersecurity Mesh Architecture and the innovative Data Security Posture Management (DSPM), LinkShadow cultivates a network of trusted advisors who are well-prepared to address the unique challenges their clients face in safeguarding sensitive information. This collaborative approach empowers partners to offer tailored solutions that align with clients' specific security needs, enhancing overall service delivery.

The channel partner program includes comprehensive training sessions, access to cutting-edge resources, and ongoing support to ensure partners remain at the forefront of cybersecurity developments. This commitment to education enables partners to effectively implement and manage LinkShadow's advanced security solutions, thereby enhancing their expertise and confidence in addressing client concerns.

Moreover, this partnership model fosters long-lasting relationships built on trust and shared goals. By collaborating closely with partners, LinkShadow not only strengthens its market presence but also creates a community dedicated to improving cybersecurity resilience. Partners are encouraged to share insights and best practices, facilitating

a continuous feedback loop that drives innovation and service enhancement.

Through this initiative, LinkShadow aims to establish a robust ecosystem of cybersecurity professionals who are empowered to proactively manage risks, respond to emerging threats, and ensure compliance with regulatory standards. Ultimately, this collaborative framework positions both LinkShadow and its partners to deliver superior cybersecurity solutions, safeguarding clients' critical assets while building a trusted foundation for future growth.

Conclusion: A Forward-Thinking Approach to Cybersecurity

In a rapidly evolving digital landscape, cybersecurity must be proactive, integrated, and adaptable to effectively address the complexities of modern threats. The Cybersecurity Mesh Architecture, coupled with the launch of the LinkShadow Data Security Posture Management (DSPM), firmly positions the company as a leader in this critical field. By emphasizing connectivity across disparate security tools, LinkShadow fosters a unified approach that enhances visibility and response capabilities. With a strong focus on Al-driven insights,

REVOLUTIONIZING CYBERSECURITY WITH LINKSHADOW'S ADVANCED AI INNOVATIONS.

organizations can anticipate threats more effectively and make informed decisions to mitigate risks.

Furthermore, LinkShadow DSPM addresses the pressing need for compliance in an increasingly complex regulatory environment. By providing organizations with comprehensive tools for automated data discovery, risk assessment, and real-time monitoring, LinkShadow not only strengthens security measures but also simplifies the compliance process. This capability is crucial for organizations striving to meet stringent regulations while safeguarding sensitive information.

As businesses face a range of cybersecurity challenges —from advanced ransomware attacks to insider threats—LinkShadow remains steadfast in its commitment to delivering innovative solutions. The company empowers organizations to protect their digital assets effectively, enabling them to focus on growth and innovation without compromising security. By fostering a culture of trust and transparency with stakeholders, LinkShadow helps businesses build resilient frameworks that are not only secure but also adaptable to future challenges.

In this dynamic environment,
LinkShadow's dedication to enhancing
security measures and enabling
organizational resilience stands out. By
continuously evolving its offerings and
investing in cutting-edge technology,
LinkShadow ensures that its clients are
well-equipped to thrive in a complex
digital world, ultimately reinforcing their
reputation and success in an era marked
by rapid change and uncertainty.



n recent years, there has been a significant increase in cyber threats targeting network infrastructure. How is D-Link addressing these challenges to enhance the security of its networking products?

At D-Link, we're deeply committed to tackling the rising cyber threats that target network infrastructure. We regularly update our firmware and release security patches to address vulnerabilities and keep our devices secure. Our newer models come with advanced security features like built-in firewalls. Intrusion Detection and Prevention Systems (IDPS), and strong encryption standards such as WPA3. We also emphasise the importance of secure configuration by encouraging users to change default passwords and use secure management interfaces. By staying on top of the latest threat intelligence and collaborating with cybersecurity experts, we ensure our products are well-protected. Plus, we provide resources to help users understand and implement best security practices. Through all these efforts, we aim to keep networks safe from evolving cvber threats.

Can you discuss any specific security features or technologies that D-Link has integrated into its latest products to protect users from cyber threats? How do these features set D-Link apart from competitors?

At D-Link, we've packed our latest products with cutting-edge security features to keep users safe from cyber threats. For starters, we've integrated Albased technology that helps detect and block suspicious activities in real-time. Our mydlink cloud platform allows you to manage and monitor your network from anywhere and keeps you updated with alerts about potential security issues. We also offer SecureSpot, a cloudbased service that provides real-time protection against malware and phishing attacks. By adopting WPA3 encryption, we ensure your wireless connections are

stronger and more secure. Our Intrusion Prevention System (IPS) actively monitors and prevents malicious activities on your network. Plus, our devices come with secure management interfaces that use encrypted protocols, and our advanced parental controls help keep your family safe online. We provide firmware updates through our website, allowing users to download and install the latest security patches as needed. These features, especially our blend of AI and cloud services, really set us apart from the competition by offering a thorough and user-friendly approach to network security.

As cyber attacks become more sophisticated, how does D-Link stay ahead in terms of research and development to anticipate and counteract emerging threats?

As cyber-attackers get more advanced in their tactics, D-Link is committed to staying ahead by investing heavily in research and development. Our dedicated security teams are constantly analysing new threats and vulnerabilities to keep our products secure. We work closely with leading cybersecurity firms and stay active in industry forums to keep up with the latest trends and best practices. By integrating advanced technologies like AI and machine learning, we can detect and respond to emerging threats in real-time. We also prioritize regular firmware and software updates to address any new vulnerabilities, and we conduct thorough

AT D-LINK, WE'VE
PACKED OUR LATEST
PRODUCTS WITH
CUTTING-EDGE

SECURITY FEATURES
TO KEEP USERS
SAFE FROM CYBER
THREATS.

in-house penetration testing to identify and fix potential weaknesses. By listening to user feedback and monitoring real-world incidents, we continually refine our security measures. Our ongoing investment in cutting-edge technologies ensures that our products are well-equipped to handle the ever-evolving challenges in cybersecurity.

How does D-Link educate and support its customers in maintaining the security of their network environments? Are there any particular resources or best practices that you recommend for ensuring robust network security?

At D-Link, we're deeply committed to helping you keep your network secure. We offer a range of online resources, including user manuals, setup guides, and video tutorials, to provide you with hands-on guidance. Our security awareness campaigns and webinars are designed to keep you informed and proactive about protecting your network. Our support team is always ready to assist with any security questions, and we regularly update you on essential practices like changing passwords and enabling encryption. Additionally, our community forums and collaborations with cybersecurity experts ensure you receive the latest tips and support to stay ahead of emerging threats.

To maintain a strong network security posture, start by updating your devices with the latest firmware and using strong, unique passwords. Protect your Wi-Fi with WPA3 or WPA2 encryption, and consider segmenting your network for added security. Keep your firewall active and explore using Intrusion Detection and Prevention Systems (IDPS) to monitor and defend against threats. Don't forget to change default settings on your devices and back up your important data regularly. Educate everyone on your network to recognise phishing attempts and be vigilant for any unusual activity. For additional protection, using a Virtual Private Network (VPN) for remote access is highly recommended. 🙎

55

www.tahawultech.com OCTOBERR 2024

BRIDGING THE SKILLS GAP

AZEEM AHMAD, FOUNDER & CEO, NETWORK BINARY, IRFAN SHAIKH, CHAIRMAN, OFFICE CONNECT GROUP OF COMPANIES AND MOHAMMED GUFRAN, DIRECTOR, OPERATIONS, NETWORK BINARY, TELL ANITA JOSEPH HOW THE COMPANY IS FOCUSED ON BUILDING A STRONG CYBERSECURITY SKILLS TALENT AND UPSKILLING THE EXISTING ONES.



he cybersecurity field is
experiencing a significant
skills shortage. How is
Network Binary working to
bridge this gap, and what
initiatives or partnerships do you have
in place to attract and develop new
talent in the region?

At Network Binary, we are keenly aware of the global and regional cybersecurity skills shortage, especially in the Middle East. We recognise that the rapid pace of digital transformation has outpaced the availability of skilled professionals to secure digital infrastructure, making it one of the top concerns for organisations in the region. Our approach to bridging this gap is multifaceted, focusing on both attracting new talent and upskilling existing professionals.

One of our key strategies is fostering a comprehensive Learning Ecosystem. This includes engaging students and professionals at various stages of their careers, starting with early cybersecurity education initiatives in collaboration with schools and universities. Through partnerships with educational institutions, we aim to introduce IT and cybersecurity fundamentals to students, building a strong talent pipeline from an early age.

In addition, we emphasise the reskilling and upskilling of professionals from various sectors. Many individuals from fields like administration, manufacturing, and hospitality have successfully transitioned into cybersecurity roles through our targeted training programs. We also actively partner with industry leaders and organisations, including our strategic collaboration with Office Connect Group, to ensure that our training programs align with the evolving demands of the market.

Our Corporate Social Responsibility (CSR) program is another critical component of our strategy. We are committed to making cybersecurity training accessible to underserved communities across the region. By offering scholarships and subsidised training, particularly to those from underrepresented regions, we aim to expand the pool of cybersecurity professionals.

Can you elaborate on the cybersecurity skills training programs offered by Network Binary? How do these programs address the current demands of the cybersecurity landscape and prepare individuals for real-world challenges?

Network Binary's cybersecurity training programs are designed to address the pressing demands of today's rapidly evolving cybersecurity landscape. Our programs are structured around real-world scenarios, ensuring that learners are well-equipped to handle complex cybersecurity challenges upon completing their training.

Our courses focus on a mix of hands-on labs, practical exercises, and simulated cyber-attacks to ensure that students experience realistic environments. Some of our flagship programs include training for certifications like Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), and Cisco Certified CyberOps. These certifications are aligned with global standards and are



WE ARE COMMITTED
TO MAKING
CYBERSECURITY
TRAINING
ACCESSIBLE TO
UNDERSERVED
COMMUNITIES
ACROSS THE REGION

highly sought after by employers across industries.

One of the unique aspects of our training is the integration of problem-solving skills and critical thinking. We engage our learners in group activities and discussions that simulate real-world cybersecurity threats, encouraging them to think on their feet. Our instructors, who are industry experts, provide guided learning pathways that not only cover theoretical knowledge but also ensure practical, job-ready skills.

www.tahawultech.com OCTOBERR 2024



We also stay closely connected to industry leaders to continuously update and adapt our programs based on current cybersecurity trends and threat landscapes. This allows us to provide up-to-date training on the latest tools and techniques, such as threat intelligence, cloud security, and Al-based cybersecurity.

What metrics or indicators do you use to measure the success and effectiveness of your cybersecurity training programs?

At Network Binary, the success and effectiveness of our cybersecurity training programs are measured through several key metrics. One of the primary indicators is certification pass rates. We track the number of students who successfully pass globally recognised certifications such as CISSP, CEH, and Cisco CyberOps after completing our training. This demonstrates their mastery of the necessary skills and knowledge.

We also measure success through post-training assessments. Learners are evaluated both before and after the training, allowing us to track progress in terms of knowledge acquisition and practical skill development. Additionally, hands-on lab performance is a critical measure, as it reflects the learners' ability to apply theoretical concepts in real-world scenarios.

Another crucial indicator is student feedback. We gather feedback through surveys and reviews, which help us continuously improve our course content and delivery. Positive feedback regarding the relevance of our training to real-world challenges is a key metric of success.

Finally, we assess the career progression of our learners. Many of our students report significant career advancement, including promotions and salary increases, after completing our programs. This is a direct measure of how well our training prepares individuals to excel in the competitive cybersecurity job market.

What are Network Binary's strategic plans for expanding its presence in the region over the next few years, and how do you intend to address the specific cybersecurity needs and challenges of this region?

Network Binary is committed to

expanding its footprint in the Middle
East and beyond by focusing on several
strategic initiatives. Over the next
few years, we plan to further diversify
our course offerings, expanding
into emerging areas like different
Verticals of AI, Data Science, cloud
security, and IoT. These technologies
are increasingly becoming integral to
businesses in the region, and we aim to
equip professionals with the necessary
skills to manage and secure them.

We also plan to strengthen our partnerships with local universities and government bodies to support the region's cybersecurity needs. By collaborating with these institutions, we aim to build a sustainable talent pipeline that meets the growing demand for skilled cybersecurity professionals.

Finally, we will continue to invest in our CSR initiatives, focusing on providing accessible cybersecurity training to underserved communities thus promoting inclusivity in social realm. This aligns with our vision of contributing to the region's long-term goals of building a secure and knowledge-driven economy.



06 - 08 MAY 2025
DUBAI WORLD TRADE CENTRE

HOSTED BY



OFFICIAL GOVERNMENT CYBERSECURITY
PARTNER



OFFICIALLY SUPPORTED BY









MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT

SCAN HERE



ENQUIRE FOR 2025!















PLATINUM SPONSORS



GOLD SPONSOR



















·I¦I·Recorded Future®

CONTACT US

⊠ gisec@dwtc.com

(3) +971 4 308 6469



#gisecglobal

MANAGING CLOUD SECURITY

SHAHNAWAZ (SHAH) SHEIKH, VP – GLOBAL SALES & ALLIANCES (CYBERSECURITY PRACTICE) AT AMISEQ, TELLS SECURITY ADVISOR HOW THE COMPANY'S CLOUD ASSESSMENT AND RELATED SERVICES ENSURE THE RIGHT CLOUD EXPERTISE TO PROVIDE THE OPTIMAL RECOMMENDATIONS OF SECURITY BEST PRACTICES.



miseq has been a leader in enterprise cybersecurity for several years. How has your approach evolved in response to the increasing sophistication of cyber threats, and what are the key strategies you recommend for organisations to stay ahead?

As the cyberthreats evolve continuously, the threat actors always find innovative ways to breach into any vulnerable areas that they become successful in identifying. We believe in recommending a strong defence, protect, respond and monitor as per the industry standard frameworks by fortifying their businesses and ensuring business continuity amidst the cyber warfare that is constantly looming. A strong cybersecurity posture is not just an IT department responsibility, it also involves leadership, users and all stake holders to be accountable and contribute with their cyber awareness roles. This synergy is crucial; technology can provide the tools and automation necessary for efficient

threat detection and response, but it is the human insight that contextualises and interprets these threats within the unique framework of each organisation.

Zero Trust Security has gained significant traction as a critical framework for protecting modern enterprises. Can you explain the core principles of Zero Trust and how Amiseq helps organisations implement this model effectively? What common challenges do companies face during this transition?

The core principles of Zero Trust is Never Trust, Always Verify, exercise least privilege and deliver continuous monitoring. Amiseg can help organisations implement this model effectively in three stages ie., starting with holistic assessment of their assets, network design, data, workload, devices etc., classifying the documents and PII information as sensitive and nonsensitive, understanding the liabilities and risks and reduce the attack surface by regulating the interfaces. Secondly help with secured transformation, get the leadership buy-in with all stakeholders on the same page supporting continuous improvement by investing in strong detection and response and aligning with digital risk management strategies. Finally, a strong detection and response in a zero-trust architecture is a critical process for time to detect and remediate for smooth functioning of businesses. Zero Trust will dramatically improve the prevention of breaches and contain the damage that can be done with any successful hack.

The common challenges companies face during this transition is as there is

a cost towards expertise, tools, services, CPU, storage and other infrastructure and to maintain, detect and respond constantly is a must and is often costly.

With the shift to cloud environments becoming more prevalent, what are the major security risks associated with cloud computing that enterprises should be aware of? How does Amiseq's cloud security solution address these risks and ensure data integrity and confidentiality?

The region has seen cloud adoption as a norm since the last few years, what's the trend these days is the multi-cloud adoption which certainly brings security and visibility concerns of their assets on the cloud. Some of the concerns that enterprises should be aware of while dealing with cloud are the following,

- a) Limited visibility and control of their data and systems on the cloud can leave businesses vulnerable to threats and misconfigurations impacting their organisation's security posture
- b) Risk related to data loss, while the cloud storage offers redundancy and resilience, one of the common cause of data loss is the ransomware attack, such attacks can encrypt or delete the data making it inaccessible to the rightful owner.
- c) Insecure API Integrations with cloud computing can pose security risks to enterprises by introducing vulnerabilities and misconfigurations that attackers can exploit. This can result in data breaches, unauthorized data modifications and compromise of cloud infrastructure.

Amiseq's cloud assessment and related services ensure the right

cloud expertise to provide the optimal recommendations of security best practices, provides visibility of all assets using Cloud Management Portals for better management of assets and business controls either on single or multi-cloud environments, provide the right recommendation of which application, workload fits best on what type of cloud infrastructure for better performance, cost, usability, security etc.,

Looking towards the future, what emerging trends or technologies do you believe will have the biggest impact on enterprise cybersecurity? How is Amiseq preparing to address these trends and incorporate them into its security solutions?

The cyberthreats continuously evolve and the volume grows with its success, the number of cybersecurity solutions to protect from such threats also continuously grow leaving many enterprise customers to be burdened with investing and managing the complexities of defence solutions to keep their businesses protected continuously. Managing this with state-of-the-art Security Operations centers and human eyes gazing at dashboards is also not very practical solution for foolproof defence. The latest trends we see is the invent of Artificial Intelligence and Intelligent Automation tools helping achieve better result round the clock even if a human eye blinks.

Amiseq is a focused professional services company, we have built our own accelerators in the form of testing lab, scripts and Intelligent Automation tools for faster and accurate deployments. These accelerators are the unique IP's of Amiseq that helps in differentiating our approach and bringing in a significant value to our vendors and customers in helping them save time to deploy and assure accuracy with a hybrid approach of human intelligence and IA tools contributing towards the best time-to-operate value to our customers. 1

AMISEQ HAS BUILT ITS OWN ACCELERATORS
IN THE FORM OF TESTING LAB, SCRIPTS AND
INTELLIGENT AUTOMATION TOOLS FOR A FASTER,
MORE SEAMLESS RESPONSE TO CYBER THREATS.

www.tahawultech.com OCTOBERR 2024 61



SETTING NEW SECURITY BENCHMARKS

AVINASH GUJJE, PRACTICE HEAD, CLOUD BOX TECHNOLOGIES, TELLS ANITA JOSEPH THAT A CONSTANTLY EVOLVING, INNOVATING SECURITY SOLUTIONS PORTFOLIO HAS POSITIONED CLOUD BOX TECHNOLOGIES WELL AHEAD OF COMPETITION.

ow is Cloud Box leveraging emerging technologies to strengthen its product/ solutions portfolio?

UAE is undergoing a significant digital transformation, driven by the adoption of AI, cloud computing, automation, and more. These technologies help businesses achieve objectives such as operational efficiency, quicker turnaround times, and cost savings. At Cloud Box Technologies, we use the latest technologies to build our product and solutions portfolio, helping us maintain a competitive edge.

By leveraging AI-driven security solutions, we enable our customers not only to detect and mitigate data breaches and cyberattacks but also to predict potential threats. This allows them to reinforce their networks and defend against future attacks and with better accuracy and speeds.

Our cloud solutions allow customers to scale their businesses according to demand, without the significant spendings in systems for on-premise infrastructure. Our use of cloudnative platforms helps our clients stay ahead of security challenges while scaling their operations without any compromises.

For more than a decade, Cloud Box Technologies has taken on various challenges. Through continuous improvement and integration of the latest technologies, our portfolio ensures that our customers remain competitive, secure, and compliant, while overcoming the security challenges that arise from the evergrowing pace of technological change.

How are emerging technologies posing a security threat to existing network infrastructure and systems, and what can organisations do to tackle these threats?

Cloud environments have been pivotal in digital transformation, providing access to resources like computing

and storage without the need for onpremise infrastructure. However, they also increase the attack surface. Weak encryption, insufficient access controls, or misconfigurations can expose stored data to threat actors.

IoT devices are designed to accomplish specific tasks and relay data but often come with inadequate security configurations, making them vulnerable to attacks like DDoS. Edge computing, another emerging technology, further expands the attack surface as data is processed closer to end users, making it harder to maintain uniform security protocols and centralised control.

To address these risks, organisations should adopt a comprehensive cybersecurity strategy that includes standardised encryption practices and continuous monitoring of connected devices and systems. Regular security audits help businesses identify vulnerabilities and fix them before threat actors exploit them. Employing a multi-lavered defence strategy. including multi-factor authentication, can also help safeguard both digital and physical assets, preventing unauthorised access and reducing the risk of security breaches reducing instances of financial and reputational losses.

What, in your experience, is the biggest security threat being faced by businesses in the region today?

Based on our 15 years of experience at Cloud Box Technologies, ransomware currently stands out as one of the most significant security threats.

These attacks particularly target high-value sectors such as finance and healthcare & can cripple organisations, resulting in financial losses, damage to reputation, downtime, and even regulatory penalties for not addressing vulnerabilities.

In the UAE, we have encountered numerous such attacks and have mitigated them by strengthening our clients' cyber defences. While the exact measures to secure a business against ransomware can vary, they generally include robust endpoint protection, access controls, and regular data backups. At Cloud Box, we also leverage AI to conduct behavioral analysis and pattern detection, which enables us to identify and prevent ransomware attacks before they happen. Our AI-driven predictive analysis, combined with strong detection and response capabilities, has proven essential in protecting businesses from such threats.

Cloud security is a huge concern for businesses today, as they seek to accelerate their digital transformation journey. How is Cloud Box stepping in to help them address this need?

As companies increasingly migrate to the cloud to remain competitive, cloud security has become a crucial issue. Many organisations fail to secure their data adequately, leading to data breaches and cyberattacks. At Cloud Box Technologies, we have developed tailored security solutions to address specific needs, rather than adopting a one-size-fits-all approach.

Our solutions include data encryption to prevent unauthorised interception of data and continuous threat detection and monitoring, which keep businesses informed about the state of their security defenses. When vulnerabilities are identified, we guide our clients on how to resolve them before it's too late. Additionally, we implement zerotrust architectures, ensuring that only authenticated users have access to specific resources, unlike traditional systems that may allow broad access across the network.

We continuously train our employees to stay abreast of emerging threats. This proactive approach allows us to protect our clients' cloud environments from all angles as they continue their digital transformation journey.

63

www.tahawultech.com OCTOBERR 2024



AI-POWERED SECURITY

TAJ EL-KHAYAT, AREA VICE PRESIDENT - SOUTH EUROPE, MIDDLE EAST, TURKEY AND AFRICA (SEMEA), TELLS SECURITY ADVISOR HOW WITH 35 PATENTS IN AI-DRIVEN THREAT DETECTION AND MORE REFERENCES THAN ANY OTHER VENDOR IN MITRE D3FEND, THE COMPANY PROVIDES ADVANCED SIGNAL INTELLIGENCE THAT SOCS CAN TRUST.

or over a decade, Vectra
Al has been researching,
developing, pioneering
and patenting its Al
security called Attack
Signal Intelligence, centered on
delivering the best attack signal on
the planet. Tell us more.

For years, cyber security has depended on well-known methods. Techniques for detecting and responding to threats have primarily relied on signatures, anomalies, and rules to detect and block cyber attackers from breaching organisations and stealing data. We believe this methodology is flawed. As enterprises transition to hybrid and multi-cloud environments, adopting digital identities, supply chains, and ecosystems, security leaders are confronted with more challenges.

There's an expanded attack surface, more ingenious and elusive attackers, more tools and datasets to assess, more signatures, anomalies, and rules to manage, increased alert noise, triage issues, false positives, and notably, analyst fatigue, burnout, and turnover. Despite having more tools, data, signatures, policies, rules, alerts, and personnel, the central issue persists: customers are still unaware of their vulnerabilities.

Vectra Security's Al-driven Attack Signal Intelligence applies a riskbased approach to cyberattacks while minimising manual workloads, alert noise, and analyst burnout. This technology enables security analysts to adopt an attacker mindset as Al-driven detections transcend traditional signatures and anomalies to comprehend attacker behaviors and reveal the entire attack narrative. By focusing on malicious activity. Aldriven Triage differentiates between harmful and benign threat activities, identifying true malicious positives while logging benign ones. With AIdriven prioritisation, critical threats are highlighted more effectively, reducing noise, automating alert triage, and

enhancing prioritisation of significant business threats by 85%.

What are some of the most pressing security challenges businesses are encountering in the current threat landscape, and how does Vectra AI tailor its solutions to address these challenges effectively?

In today's landscape, identity plays a central role in both enterprises and hybrid attacks. Attackers frequently exploit identities as entry points or to navigate networks, accessing sensitive data and deploying ransomware. According to Gartner, "Effective ITDR must detect changes in security posture (as part of hygiene) and ongoing attacks." Vectra Al identifies two types of ITDR solutions: those focused on preventing compromises by enhancing identity posture, and those detecting attackers post-compromise. Most ITDR tools concentrate on pre-compromise identity enhancement with limited postcompromise capabilities. However, few solutions address both stages comprehensively.

Security teams need visibility into both human (customers, employees, vendors, partners) and non-human identities (workloads, devices) across data centres, networks, and cloud environments. While many solutions claim to detect attack behaviors and compromised identities, it is crucial for security teams to evaluate the depth of detections along the attack path, distinguishing between anomaly-based and behavior-based detections.

VECTRA SECURITY'S AI-DRIVEN ATTACK SIGNAL INTELLIGENCE APPLIES A RISK-BASED APPROACH TO CYBERATTACKS.

Based on these insights, key criteria for selecting the right ITDR tool include Coverage to reduce exposure, Clarity to eliminate latency, and Control to optimise resources. The Vectra AI Platform addresses over 90% of MITRE ATT&CK techniques, including post-compromise methods, thereby reducing exposure and cutting through noise better than traditional UEBA solutions. It also allows for customised prioritisation rules, offering clarity on real attacker behaviors and freeing up resources for other tasks. Notably, Vectra Al's response capabilities provide native, integrated, and managed responses. Native responses enable automatic account lockdowns and session revocations, stopping compromised identities or associated endpoints on the platform. Customised responses minimise operational disruptions while investigating identities.

Organisations at varying stages of identity security maturity should prioritise selecting post-compromise focused ITDR solutions for their SOC. Security Leaders, Architects, Engineers and Analysts are advised to evaluate vendors based on outcomedriven criteria and involve multiple stakeholders, including GRC and IAM teams, in the decision-making process.

How does Vectra AI handle the challenge of dealing with false positives and ensuring the relevancy of threat alerts in a rapidly evolving cyber threat environment? What strategies are in place to minimise alert fatigue and improve the overall accuracy of threat detection?

Vectra Al-driven Attack Signal
Intelligence reveals the complete
dynamics of an attack, offering your
analysts unparalleled signal clarity that
enables your SOC team to concentrate
on the most pressing and severe
threats. Equipped with Al-driven
Prioritisation features, it automates the
process of prioritising alerts for every

65

www.tahawultech.com OCTOBERR 2024



detection, providing SOC teams with an effective method to allocate resources toward what is most critical for the business. Here's how it works:

- Al-Driven Prioritisation incorporates Attack Velocity – It precisely determines and evaluates the speed of attack progression, which is crucial when assigning urgent priority in the risk scoring mechanism where timing is vital.
- Comprehensive role understanding

 Using substantial behavior based models, it helps in
 thoroughly grasping the roles and
 permissions of each end-user in
 your organisation, allowing prompt
 identification of anomalies.
- Accurate incident scoring Vectra
 Al aggregates inputs from all data
 sources across various domains to
 identify behaviors leading to serious
 and advancing incidents.
- Customisable scoring methods -

- Your SecOps team can set priorities based on key assets and critical entities pertinent to your business, ensuring these are primary factors in determining incident priorities.
- Counteract attackers Vectra
 Al-Driven Detections identify up to
 90% of tactics and techniques from
 the MITRE ATT&CK framework,
 enabling your SecOps team to
 anticipate and counter attackers'
 strategies.
- Enriched context from all data sources – Vectra Al provides a comprehensive view of the entire attack scenario, emphasising the gravity of incidents to ensure accurate incident response.

In light of the increasing complexity of cyber attacks, how does Vectra AI's approach to threat detection and response evolve to keep pace with new attack vectors and techniques?

Vectra AI has a team of security researchers with domain expertise across network, identity, and cloud (laaS, PaaS, SaaS) that stay on top of evolving attack surfaces and emerging attacker techniques. At the same time, the global Vectra MDR team of analysts monitor customer environments identifying new attacker methods in the wild. The combination of security research and real-world monitoring of attacker behaviors enables our data scientists to develop new AI detection algorithms and roll out to customers in less than two weeks.

Vectra AI has more patents in AI-driven threat detection than any other cybersecurity company on the planet. With 35 patents in AI-driven threat detection and more references than any other vendor in MITRE D3FEND, we provide advanced signal intelligence your SOC can trust. 1





Copilot+ PCs

Surface Pro and Surface Laptop deliver the best of AI across devices and the cloud to drive productivity, creativity, innovation, and resilience. To ensure a seamless experience, we built and tested Copilotand Copilot for Microsoft 365 on Surface devices.

Surface Pro

Pioneering versatility matched by intelligent power

Unlock high performance in a form factor that redefines what a laptop can do.





The HD front-facing Surface Studio Camera supports powerful Windows Studio Effects.



Employees interact with Copilot effortlessly through touch gestures or inking with Surface Slim Penon the PixelSense™ Flow touchscreen.



The new Copilot key provides access to Copilot.

On-device AI finds almost anything fast with Recall and empowers collaboration through real-time translation of 40+ languages to English using Live Captions.



Snapdragon®X Elite and Plus processors unlock new levels of speed and efficiency with an industry-leading NPU that drives up to 45 TOPS for seamless on-device AI.



Surface Laptop

Transformative design packed with intelligent power

Embrace opportunity with Copilot+ PC performance in a newly sleek profile with a smaller footprint and larger screen real estate.



+973 17700777 acsales@almoayyedcomputers.com www.acme.tech

APROACTIVE APPROACH TO RISK MANAGEMENT

ROHAN DANIEL NAIR, FOUNDER & CHIEF OPERATING OFFICER AT AHAD, TELLS ANITA JOSEPH HOW THE COMPANY COMBINES INNOVATION & TECHNOLOGY TO OFFER PROACTIVE DEFENCE SOLUTIONS AGAINST THE MOST SOPHISTICATED THREATS.

n today's rapidly evolving digital landscape, what are the most pressing cybersecurity challenges organisations in the region face, and how is AHAD addressing these challenges through innovation and technology?

In today's rapidly evolving digital landscape, organisations face increasingly sophisticated cyberattacks, including ransomware, phishing, and insider threats, as well as the challenges of regulatory compliance and data privacy. AHAD tackles these pressing cybersecurity issues through innovation and technology by offering end-to-end offensive security, intelligence, and strategic advisory services. Our advanced Cyber Defense Center delivers proactive defence solutions like attack surface management, deep

and dark web monitoring, and AI-driven threat intelligence. By focusing on early detection, rapid response, and comprehensive risk assessments, we ensure organisations stay resilient and secure in this complex threat environment.

Digital transformation is a key trend in modern business. How does AHAD help organisations navigate the cybersecurity risks associated with this transformation, and what strategies do you recommend for ensuring a secure transition?

Digital transformation reshapes the way businesses operate, but it also introduces new cybersecurity risks, from cloud vulnerabilities to complex threat landscapes like AI-driven attacks. At AHAD, we guide organisations through

these risks with a holistic, security-first approach to digital transformation. Our expertise in digital forensics, incident response, and offensive security ensures that as businesses adopt new technologies, they remain protected against emerging threats. We recommend a strategy focused on continuous risk assessment, robust endpoint detection, and proactive defense through AI-driven threat intelligence. By implementing zero-trust architectures and advanced compliance frameworks, AHAD ensures that businesses can embrace digital transformation securely while maintaining regulatory compliance and operational resilience.

Effective risk management is crucial for minimising vulnerabilities. Can you elaborate on AHAD's approach to risk management and how your solutions help clients identify, assess, and mitigate potential risks?

At AHAD, our approach to risk management is comprehensive and proactive, focusing on minimizing vulnerabilities through continuous assessment and actionable insights. We

OUR EXPERTISE IN DIGITAL FORENSICS, INCIDENT RESPONSE, AND OFFENSIVE SECURITY ENSURES THAT AS BUSINESSES ADOPT NEW TECHNOLOGIES, THEY REMAIN PROTECTED AGAINST EMERGING THREATS.



begin with in-depth security assessments to identify gaps, followed by threat modelling and real-time monitoring to assess potential risks. Using our advanced Cyber Défense Centre, we offer clients unparalleled visibility into their attack surface, combined with deep and dark web monitoring to pre-emptively identify threats. Our intelligence-driven solutions not only detect vulnerabilities but also prioritise them based on their criticality. This enables rapid mitigation through strategies like endpoint detection, response automation, and zero-trust architectures. By integrating these with compliance frameworks, AHAD ensures that organisations not only manage risk but also strengthen their overall cybersecurity posture.

With the cybersecurity landscape constantly evolving, what emerging threats or trends do you foresee in the near future, and how is AHAD preparing to address these new challenges?

The cybersecurity landscape is rapidly evolving, and emerging threats like Aldriven attacks, advanced ransomware, and nation-state espionage are becoming more sophisticated. We also see increasing threats from social engineering and insider risks, with over 98% of attacks now leveraging social engineering techniques. AHAD is at the forefront of

tackling these challenges by staying ahead of the curve through continuous innovation. Our Cyber Défense Centre is designed to proactively detect and neutralise threats before they become incidents. We focus on Al-powered threat intelligence, dark web monitoring, and advanced endpoint protection to stay agile in this shifting environment. Additionally, our offensive security capabilities allow us to simulate future attack vectors. ensuring that our clients are prepared for tomorrow's threats. With our expertise in regulatory compliance and risk management, AHAD helps organisations remain resilient and secure in an increasingly complex digital landscape. 🚦

www.tahawultech.com OCTOBERR 2024 **6**

COMPROMISED ACCOUNTS, CUSTOMISED SOCIAL ENGINEERING USED TO TARGET TRANSPORT AND LOGISTICS FIRMS WITH MALWARE

roofpoint researchers are tracking a cluster of activity targeting transportation and logistics companies in North America to deliver a variety of different malware payloads.

Notably, this activity leverages compromised legitimate email accounts that belong to transportation and shipping companies. At this time, it is unclear how the actor achieves access to the compromised accounts. The actor then injects malicious content into existing conversations within the account's inbox, which makes the messages look legitimate. Proofpoint has identified at least 15 compromised email

accounts used during these campaigns.

Researchers have been tracking this activity cluster since late May 2024.

Activity which occurred from May to July 2024 predominately delivered Lumma Stealer, StealC, or NetSupport. In August 2024, the threat actor changed tactics by employing new infrastructure and a new delivery technique, as well as adding payloads to deliver DanaBot and Arechclient2.

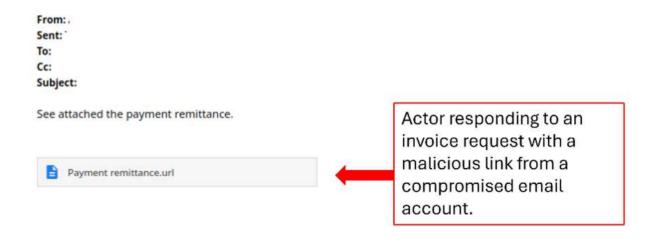
Most campaigns use messages with Google Drive URLs leading to an internet shortcut (.URL) file, or a .URL file attached directly to the message. If executed, it uses SMB to access an executable from the remote share, which

installs the malware.

Campaigns typically include less than 20 messages and impact a small number of customers, all in the same transport/logistics industries in North America.

In August 2024, the actor also began using the "ClickFix" technique to deliver their malware. The messages contained URLs which directed users through various dialogue boxes leading them to copy, paste, and run a Base64 encoded PowerShell script contained within the HTML, a technique called "ClickFix." The scripts led to an MSI file used to load DanaBot.

While Proofpoint has observed this technique leveraged by other threat



On Mon, Good morning wrote:



actors impersonating Word or Chrome updates, these campaigns have impersonated Samsara, AMB Logistic, and Astra TMS – software that would only be used in transport and fleet operations management.

Attribution

Proofpoint does not currently attribute this activity cluster to an identified threat actor (TA). Similar techniques and infrastructure associated with ClickFix and the combination of Google Drive URLs, .URL files, and SMB have been observed used by other threat actors and campaigns. Proofpoint researchers assess that the threat actor discussed in this Security Brief is purchasing this infrastructure from third party providers.

Based on the observed initial access activity, malware delivery, and

infrastructure, Proofpoint assesses with moderate confidence the activity aligns with financially motivated, cybercriminal objectives.

Why it matters

Threat actors are increasingly tailoring lures to be more realistic to entice recipients to click on a link or download attachments. Compromising legitimate email accounts and sending malicious links and attachments to an existing email conversation achieves this goal and raises the risk that recipients will install malware.

The specific targeting and compromises of organisations within transportation and logistics, as well as the use of lures that impersonate software specifically designed for freight operations and fleet management,

indicates that the actor likely conducts research into the targeted company's operations before sending campaigns. The language used in the lures and content also indicate familiarity with typical business workflows.

This activity aligns with a trend Proofpoint researchers have observed across the cybercriminal threat landscape. Threat actors are developing more sophisticated social engineering and initial access techniques across the delivery attack chain while relying more on commodity malware rather than complex and unique malware payloads.

Members of the transportation/
logistics industry, and users in general,
should exercise caution with emails
coming from known senders which
deviate from normal activity or content,
particularly when combined with unusual
looking links and file types such as
described in this Security Brief. In other
words, emails that do not look or feel
right and trigger a sixth sense that
something is off.

When encountering such activity users should contact the sender using another means to confirm their authenticity. 1

CAMPAIGNS TYPICALLY INCLUDE LESS THAN 20 MESSAGES AND IMPACT A SMALL NUMBER OF CUSTOMERS, ALL IN THE SAME TRANSPORT/LOGISTICS INDUSTRIES IN NORTH AMERICA.

www.tahawultech.com OCTOBERR 2024

FIND THE BALANCE FOR GENAI USAGE IN THE WORKPLACE OR RISK SECURITY THREATS: KASPERSKY

enerative Artificial Intelligence (GenAI) tools are quickly becoming an integral part of the modern work environment. fulfilling a range of professional tasks from drafting a report to analysing spreadsheets, amongst others. A global Kaspersky survey found that 95% of C-suite respondents are aware that GenAl tools are used within their organizations with more than half (59%) being concerned about the risks of employees inadvertently leaking sensitive information when using Al. Kaspersky experts give advice how organizations can use GenAl tools in a risk-adverse way.

"GenAl tools are enabling employees to become more productive as the technology assists with data analysis and routine tasks. Yet, many people are using Al without proper authorisation from their employer," says Vladislav Tushkanov, Machine Learning Technology Group Manager at Kaspersky. "This could hold significant risks for the organisation. For instance, data leakage remains a significant concern. Furthermore, employees can get and act upon wrong information as a result of 'hallucinations.' This is when large language models present false information in a confident way. These hallucinations can be especially dangerous when GenAI is used to provide advice on how to complete certain work functions."

Addressing this challenge is now a business imperative. Another Kaspersky survey has revealed that 40% of

kaspersky

respondents from the UAE now see Al as a team member at work. Adding complexity to this is how effectively malicious users have adopted GenAl tools to create more convincing social engineering attacks to target individuals. For instance, drafting personalised phishing emails; generating deepfakes that contain realistic audio, video, or text content that impersonates people; and even propagating disinformation campaigns that can influence public opinion or obscure the truth.

"This does not mean that organisations should block GenAl completely. Instead, decision-makers must conduct a comprehensive risk assessment to understand which parts of the daily business routine can be automated with GenAl tools without adding to the threat level facing the business," says Tushkanov.

Through this, organisations can adopt a centralized approach when it comes to GenAl adoption. Such a service can then be provided via an enterprise account with a cloud provider while ensuring all the necessary safeguards are in place. These can include monitoring for potential personally identifiable information in messages as well as

oversight. Organisations should also educate employees on the acceptable use of GenAl and the proper, companymanaged, ways of accessing them.

By understanding the benefits and risks of using GenAl and ensuring the necessary security measures are in place to mitigate any potential dangers, organisations can significantly improve employee productivity while also increasing job satisfaction. General rules for employees should include not disclosing confidential data to AI tools; not relying on their advice for any critical use case; verifying information; remembering that data provided to a chatbot can leak. And that all computers and servers running large language model (LLM) based systems are protected with up-to-date security tools.

"Simply banning tools like ChatGPT and other solutions might be not the best option. GenAl can be used positively by finding the balance between too much and too little caution. More broadly, partnerships between the public and private sector can see GenAl becoming a critical enabler to help drive business growth, enable more resources spent on innovation, and adequately manage risk," said Tushkanov.



14 - 18 OCT 2024 DUBAL WORLD TRADE CENTRE

11 AM - 5 PM

TUE - FRI 10 AM - 5 PM

THE LARGEST TECH & AI SHOW IN THE WORLD

Global Collaboration to Forge a Future Al Economy



Connecting you to new business opportunities in the world's most profitable digital ecosystems

6,500+ **Exhibitors**

200,000+ **Tech Executives**

180+ Countries

#GITEXGLOBAL gitex.com









Scan the QR code to **SECURE YOUR PASS**







Data Security Posture Management

— From On-Prem to Multi-Cloud



GITEX GLOBAL STOP BY HALL #25-C60 14-18 OCT 2024 E: info@linkshadow.com

T: +1 877 267 7313

W: linkshadow.com