ADVISOR

MIDDLE EAST

SECURING BECURING BEC

computer news middle east SUPPLEMENT

🔅 tahawultech.com



Keep an eye on your home from anywhere

Video doorbells, security cameras and alarm system

Ring lets you monitor every corner of your property. With a Video Doorbell at your door and Security Cams around the house, you can create a Ring of Security around your entire home.

Ring... smart security for every home.



Available at:	Dubai	MYZ	DSR Tech	AL Ershad	Hyper X	Innox	Zoomline
		Tel: +971 4 351 1825	Tel: +971 4 238 0921	Tel: +971 4 359 8896	Tel: +971 4 352 8820	Tel: +971 4 386 1418	Tel: +971 4 325 7866
	Abu Dhabi	Royal Phone Center	Empower / Apple Plus	s Computers			
		Tel: +971 2 491 8888	Tel: +971 2 445	3222			

CONTENTS









6 News roundup from the world of security in the region and beyond.

12 SECURING THE FUTURE

10 Findings from the OPSWAT survey which reveals that only 2% of organizations feel confident with current security strategies.

22 Kevin Kennedy of Vectra AI on how security analysts in UAE & KSA fear they are missing a relevant security event.

26 Insights into how Kyndryl and Veritas have introduced new solutions for Data Protection and Recovery.



-0

Secure Your Digital Future Simple. Secure. Resilient.

Secure Your Enterprise IT Footprint For A Safer Digital Journey

> www.raqmiyat.com UAE | KSA | INDIA



EDITOR'S NOTE



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

> Anita Joseph Editor

EVENTS



FUTURE OF CYBERSECURITY

Dear Readers,

Welcome to the latest edition of your favourite cybersecurity magazine, where we delve into the ever-evolving intersection of artificial intelligence and cybersecurity. As technology continues to push the boundaries of innovation, the integration of AI in the cybersecurity landscape has emerged as a game-changer in safequarding our digital world.

In this issue, we embark on a journey to explore the myriad ways in which AI is

reshaping the cybersecurity landscape. From threat detection and prevention to incident response and recovery, AIpowered solutions have proven their worth in fortifying our defenses against sophisticated cyber adversaries.

As the cybersecurity landscape grows increasingly complex, the need for advanced technologies becomes more evident than ever before. AI, with its ability to analyze vast volumes of data in realtime, offers unparalleled insights into potential threats, enabling us to stay one step ahead of cyber attackers.

However, with every technological advancement, there are also challenges and ethical considerations that deserve our attention. Throughout these pages, we also address the potential risks associated with the use of AI in cybersecurity, ensuring that we approach these cuttingedge technologies with a responsible and cautious mindset.

We are honored to feature opinions and perspectives from experts in both AI and cybersecurity fields, who share their invaluable perspectives on the current

SECURITY & TECHNOLOGY

state and future prospects of Al in strengthening our digital defenses. Their insights shed light on how Al is empowering

security professionals to mitigate risks and respond to cyber incidents with unprecedented speed and accuracy.

As we continue to explore this fascinating realm of AI and cybersecurity, we encourage you to join the conversation. Share your thoughts, experiences, and concerns with us as we navigate this dynamic landscape together.

Thank you for your continued support and for being a part of our cybersecurity community. We hope this edition leaves you informed, inspired, and prepared to embrace the opportunities that AI presents while maintaining a vigilant approach to safeguarding our digital world.

Published by

Stay secure!

FOUNDER, CPI Dominic De Sousa (1959-2015)

ADVERTISING Group Publishing Director Kausar Syed kausar.syed@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.joseph@cpimediagroup.comm

PRODUCTION AND DESIGN Designer Prajith Payyapilly prajith.payyapilly@coimediagroup.com DIGITAL SERVICES Web Developer Adarsh Snehajan webmaster@coimediagroup.com Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai, UAE Tel: +971 4 5682993

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com daniel.shepherd@cpimediagroup.com

OnlineEditor

Daniel Shenherd

Veronica Martin Contributing Editor SAME & Tahawultech.com All rights reserved While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

© Copyright 2023 CPI

MANAGEENGINE SITE24X7 UNVEILS OPENAI OBSERVABILITY INTEGRATION FOR ENHANCED PERFORMANCE MONITORING

ManageEngine, the enterprise

IT management division of Zoho Corporation, announced that it has newly added OpenAI observability as a native capability to Site24x7, its comprehensive cloud-based observability platform. The offering enables application owners to monitor the utilisation of different OpenAl models seamlessly while tracking real-time performance and cost metrics — all within a unified view. This powerful capability empowers businesses to leverage the potential of emerging AI technologies, such as OpenAl's ChatGPT, to drive innovation and achieve their strategic objectives while being cost-conscious.

embrace OpenAI's latest generative AI model and explore the potential of ChatGPT across multiple teams, gaining a comprehensive understanding of user interactions with GPT-powered applications becomes crucial. This understanding enables the identification of valuable opportunities to optimise models and enhance user experiences. Additionally, closely monitoring API usage and token consumption becomes essential to managing costs and enhancing overall application performance.

"As the demand for OpenAI's GPT-4 model continues to soar, companies are compelled to reimagine and revamp their existing service landscapes to



enhance the user experience," said Srinivasa Raghavan, director of product management for Site24x7. "Observability emerges as a transformative force, empowering companies to get the most out of GPT. Our commitment to enabling organisations using GPT APIs is reflected in our efforts to provide effortless setup, cost and performance monitoring. We aim to ensure that efficiency and effectiveness remain at the forefront of our AI-driven IT operations management solution."

As organisations increasingly

HUAWEI CLOUD RELEASES PANGU 3.0

Huawei is bringing forth new

industry opportunities and technological advancements driven by the Al wave. During his keynote speech at Huawei's Developer Conference, Zhang Pingan, Huawei Executive Director and CEO of HUAWEI CLOUD, unveiled the Pangu Model 3.0 and Ascend Al cloud services. These innovations aim to empower industry customers and partners and unlock the potential of artificial intelligence for transformative growth across a range of sectors.

Pangu Models 3.0 is a system of pre-trained models that can be quickly adapted to meet scenario-specific needs and address complex challenges across multiple industries. By leveraging large-scale data sets and machine



learning algorithms, Pangu 3.0 is set to revolutionise the industrial application of AI in diverse areas such as weather forecasting, drug development, fault identification in trains, and the mining industry.

"Pangu should enable every industry, every enterprise and everyone to have their own expert assistant so that work is more efficient and easier. We always adhere to the Al for industries strategy and continue to move forward on deepening into vertical industries. I firmly believe that large models will reshape every industry, and every developer will become a world-changing hero." said Zhang Pingan.

Prestigious science journal Nature recently published a paper describing

the enormous potential that artificial intelligence holds for weather prediction. The paper described how Huawei's Pangu Meteorology Model team developed a precise and accurate global AI weather forecast system based on deep learning using 43 years of data.

CHAINALYSIS RESEARCH FINDS CRYPTOCURRENCY CRIME DOWN 65% YEAR-TO-DATE

The outlook of global crypto markets,

which have been recovering well this year with the prices of digital assets like Bitcoin up over 80% as of June 30, has been infused with further positivity following the release of the latest Crypto Crime Midyear Update from Chainalysis. This research shows that cryptocurrency inflows to known illicit entities1 have declined by a staggering US\$5.2billion (a 65% decrease) compared to the same time last year, while inflows to risky entities such as high-risk exchanges and crypto mixers are down 42%.

Encouragingly, inflows to illicit addresses are down in nearly every category of crypto crime — from hacks and malware to fraud shops and darknet markets — with the decline in scam revenues being the most significant. As of June, crypto scammers have taken in nearly US\$3.3 billion less (at 77% decline) in 2023 than they did in 2022, for a total of just over US\$1.0 billion this year. This decline is especially impressive given that last year, crypto scam revenues had already dropped by 46%.

"After a chaotic 2022 which saw significant volatility and the high-profile collapse of FTX, it is reassuring to see confidence return to the crypto markets as asset prices are largely on the rise, and the volume of crypto crime has dropped significantly," said Kim Grauer, Director of Research at Chainalysis. "This bodes especially well for the UAE, where the government remained



fervently committed to its vision of establishing the country as a global crypto hub even through challenging times. These efforts — which include the establishment of the VARA and the introduction of comprehensive regulations for VASPs — ensure that as momentum returns to crypto markets, the country stands out as being especially attractive to businesses, entrepreneurs and investors."

JUNIPER NETWORKS' AI-DRIVEN WIRELESS TAKES DIGITAL EXPERIENCE TO A NEW LEVEL AT THE UNIVERSITY OF OXFORD

Juniper Networks, a leader in secure,

Al-driven networks, announced that numerous departments and colleges of the University of Oxford, a renowned university and the oldest centre of learning, teaching and research in the English-speaking world, deployed Juniper's cloud-delivered wireless access solution driven by Mist Al to provide a modern digital experience to students, faculty, staff and guests.

The University of Oxford strives to deliver a platform that underpins education, research and personal connectivity, enhancing the day-to-day life of the university community. The university invests in its technology infrastructure to enable all staff, students and guests to communicate effectively, share information and



collaborate widely. Oxford's new Aldriven Wi-Fi from Juniper supports central administration, libraries, student rooms, colleges and department buildings, optimising the user experience for many students, staff and visitors.

The University's departments and colleges that deployed the Juniper Wireless LAN solution, driven by Mist AI, streamlined network operations and delivered predictable, reliable and measurable user experiences in key administrative buildings, libraries, student rooms and colleges. Juniper's cloud-delivered services, including Juniper Mist Wireless Assurance and Marvis Virtual Network Assistant, give the IT staff unique insight into individual user experiences. It also accelerated deployment, as well as the management and troubleshooting of Wi-Fi with unique Al-driven operations, including automated event correlation, predictive analytics and self-driving network operations.

TRELLIX LAUNCHES CISO COUNCIL WITH TOP CYBERSECURITY EXPERTS

Trellix, the cybersecurity company

delivering the future of extended detection and response (XDR), has announced its new Mind of the CISO initiative, bringing global attention to the needs of the CISO community. The collaborative efforts span an inaugural CISO Council, research, and webinars.

Trellix's CISO Council is founded on the principle of information sharing. The council brings together global influential experts to educate the industry on the challenges and solutions needed to effect change. Members will participate in Trellixhosted events around the world and will also provide insightful contributed content.

"CISOs face new challenges resulting from the rapidly changing threat landscape, the advents of AI and other disruptive technologies, and regulatory changes," said Harold Rivas, CISO at Trellix. "As chief defenders, we must actively collaborate



with our peers to identify successful ways to navigate these challenges. Collaboration is one of the most potent tools we have."

According to Trellix's 2023 Mind of the CISO research, the top challenges CISOs face are too many sources of information, the changing regulatory landscape, a growing attack surface, and the lack of skilled talent on their teams. AI is the newest change they need to navigate. Cybercriminals use AI to hone their skills while Security Operations teams benefit from automation and insights. To ensure a level playing field between good and bad actors, Trellix supports CISOs' effective use of their current tools and shape future solutions.

TENABLE JOINS CLOUD SECURITY ALLIANCE

Tenable, the Exposure Management

company, has announced that it has joined the Cloud Security Alliance (CSA) as Executive Member. CSA is the world's leading organisation dedicated to defining standards, certifications and best practices to help ensure a secure cloud computing environment.

As an executive level member. Tenable will champion preventive security approaches, helping organisations understand and reduce cybersecurity risk across their entire attack surface—from the cloud, IT, OT, identity systems and beyond. Tenable brings a wealth of expertise in cloud exposure management, having helped thousands of organisations maintain security and compliance standards without slowing down development cycles. Tenable Cloud Security enables organisations to continuously assess the security posture of cloud environments, offering full visibility across multi-cloud environments and helping organisations prioritise security efforts based on actual risk.



"According to a study conducted by Forrester Consulting on behalf of Tenable, 64% of businesses already use cloud security tools as part of their overall cybersecurity strategy1," said Brian Goldfarb, chief marketing officer, Tenable. "But the speed and scale of cloud computing often leave environments riddled with undetected or unpremediated exposures such as misconfigurations, vulnerabilities and excess privileges. Joining CSA is an important way for Tenable to engage with cloud users and collaborate with our industry peers on important initiatives so we can secure these complex environments before they can be exploited by cyber attackers."

DELINEA NAMED GROWTH LEADER IN PRIVILEGED ACCESS MANAGEMENT BY FROST & SULLIVAN



Delinea, a leading provider of solutions that seamlessly extend Privileged Access Management (PAM), has announced it has been recognised as a Leader in the 2023 Frost Radar for PAM report. The Frost & Sullivan report, which evaluated 12 vendors, found that Delinea is the top Leader in the Growth Index.

"Delinea has topped the Frost Radar Growth Index because of their consistent and strong financial performance in terms of revenue and market share growth in the global PAM market during the last 3 years," the report summarises. The Frost & Sullivan report also indicates that Delinea's extensive customer base, strong market presence across different verticals, investment efforts in expanding global reach, and large channel partner ecosystem and programs contributed to its recognition as a Growth Leader. "We believe that Delinea's Leader placement in the Frost Radar Growth Index underscores the investments that we're making to address the expanding privileged access requirements of global businesses of all sizes, across all industries," said Art Gilliland, CEO at Delinea. "Our solutions are known for being seamless and usable to help keep organisations secure and quickly realise the value of the investment. We are proud to come out on top in the Growth Index and as an Innovation Leader in the 2023 Frost Radar for PAM "

Allied Telesis



Next Generation Industrial Switches

Our award winning family of IE switches just got better thanks to the IE220 Series

10 Gigabit uplink ports gives you the value and versatility your network requires. The ideal speed where high bandwidth backhauling and scalability is required. Coupled with IEEE 802.3bt PoE++ up to 95W to meet the demand for high power of devices connected to the network – this really is built for enduring performance in the harshest of environments, such as those found in outdoor installations. With rich functionality and advanced security features, our switches deliver the performance and reliability demanded by deployments in the age of the Internet of Things.

For more information, please contact one of our Allied Telesis Account Managers today.



Tel: +971 4 3522 433

OPSWAT SURVEY REVEALS ONLY 2% OF ORGANIZATIONS FEEL CONFIDENT WITH CURRENT SECURITY STRATEGIES

6

.



PSWAT, a global leader in critical infrastructure protection (CIP) cybersecurity solutions. released the findings of its 2023 State of Web Application Security report, based on an online survey of over 400 executive leaders, managers, and senior contributors. The survey provides a deep dive into the evolving state of web applications and cloud infrastructure and highlights a concerning disconnect: While 75% of organizations have made significant strides to upgrade their infrastructure in the past year, including the adoption of public cloud hosting and containerization, and 78% have increased their security budgets, only 2% of industry experts are confident in their security strategies.

In today's rapidly evolving landscape of web application security, organizations are constantly striving to adapt and fortify their infrastructure, particularly with the rise of hybrid work environments. Recognizing the need for enhanced productivity and scalable solutions, most organizations have embraced public cloud hosting for their web applications, with an overwhelming 97% already employing or planning to implement containerization.

The use of applications utilizing storage services has also increased with these infrastructure upgrades, elevating concerns around file-based malware.

Key Research Findings: 62% of organizations use five or less antivirus (AV) engines to detect malicious file uploads

 This indicates a potential vulnerability, as deploying more engines can significantly strengthen an organization's defense against advanced malware.

Large organizations are more likely to use Content Disarm and Reconstruction (CDR)

 This trend can be attributed to the higher volume of files handled by these organizations, making them more susceptible to cyberattacks. However, small and medium-sized organizations can also greatly benefit from adopting CDR as a proactive measure against evolving cyber threats.

98% of organizations would benefit from additional prevention-based approaches

 These include periodic analysis of all file repositories in their web applications for malware, detection of vulnerabilities in running virtual machine containers, and prevention of data exfiltration by redacting or blocking sensitive data.

"Irrespective of the size or industry, organizations must recognize that infrastructure upgrades alone are not sufficient to guarantee robust security," said Yiyi Miao, Chief Product Officer at OPSWAT. "It is imperative to establish a proactive defense strategy that goes beyond traditional measures. By adopting and combining advanced threat prevention technologies like multi-AV scanning, CDR, DLP and dynamic threat analysis, organizations can effectively establish multiple lines of defense against known and unknown emerging threats and safequard their critical infrastructure."

SECURING THE FUTURE

IN THE DIGITAL AGE, THE PARTNERSHIP BETWEEN ARTIFICIAL INTELLIGENCE AND CYBERSECURITY HAS EMERGED AS THE FRONTLINE DEFENSE AGAINST CYBER THREATS. WE EXAMINE HOW THIS DYNAMIC PLAYS OUT AND WHAT THE FUTURE OF CYBERSECURITY LOOKS LIKE.

$\rightarrow \begin{array}{l} \mbox{While al Can Automate Many Cybersecurity} \\ \mbox{Tasks, it cannot completely replace} \\ \mbox{Human expertise and Judgment.} \end{array}$

its shadows. In this article, we delve into the symbiotic relationship between AI and cybersecurity, exploring how this dynamic duo is bolstering our defenses against a relentless tide of cyber threats.

The Cybersecurity Landscape: A Perpetual Battlefield

In today's interconnected world, data has become the new currency, and as a result, cyber threats have grown more sophisticated, pervasive, and damaging than ever before. Cybercriminals, hackers, and state-sponsored actors are continually devising new strategies to breach defenses, steal sensitive information, disrupt services, and wreak havoc on individuals, organizations, and even nations. The sheer volume of attacks, combined with the speed at which they can be executed, has overwhelmed traditional security measures.

To combat this cyber warfare, organizations must employ innovative

and adaptive approaches that can match the attackers' capabilities. Enter Artificial Intelligence - an ingenious tool that offers a game-changing advantage in the battle for cybersecurity.

Al in Cybersecurity: A Match Made in Digital Heaven

At its core, AI is about empowering machines to learn from experience, identify patterns, and make intelligent decisions without explicit programming. These characteristics make AI a natural ally for cybersecurity professionals, as it can process vast amounts of data at incredible speeds, recognize subtle anomalies, and adapt to emerging threats in real-time.

Threat Detection and Prevention

Traditional cybersecurity systems often rely on rule-based approaches that can only identify known threats. This limitation makes them susceptible to zero-day attacks and novel strategies employed by cybercriminals. AI, on the other hand, utilizes advanced algorithms like machine learning and deep learning to analyze historical data, identify patterns, and predict potential future threats.

Machine learning models can be trained on massive datasets containing examples of both benign and malicious

n the ever-evolving landscape of technology, the rise of Artificial Intelligence (AI) has been nothing short of revolutionary. With its immense potential to transform industries and improve countless aspects of our lives, AI is making an undeniable impact on cybersecurity. As the digital realm becomes increasingly pervasive, so do the threats that lurk in activities. This process equips AI systems with the ability to detect and block new and unknown threats by recognizing patterns and behaviors that might indicate malicious intent. Such adaptive threat detection helps in mitigating attacks before they can exploit vulnerabilities.

Cyber Defense and Response

Al-powered cybersecurity solutions also bolster defensive measures by automating incident response. When a security breach is detected, Al systems can take immediate action to quarantine affected areas, isolate compromised devices, and deploy countermeasures. This automated response significantly reduces the response time, limiting the extent of damage and preventing the spread of malware or other malicious activities.

User Authentication and Access Control The traditional username and passwordbased authentication methods have proven to be increasingly vulnerable to hacking attempts. AI can enhance authentication processes through multi-factor authentication, behavioral biometrics, and facial recognition, making it harder for unauthorized entities to gain access to sensitive systems or data. Phishing and Social Engineering Defense

Phishing and social engineering attacks prey on human vulnerabilities, making them challenging to prevent solely through technical measures. However, Al can analyze email patterns, identify suspicious links, and assess content to differentiate between legitimate and malicious messages. By alerting users to potential phishing attempts, Al helps fortify the human firewall.

Threat Hunting and Intelligence Gathering

Al systems can comb through vast



amounts of unstructured data across the internet to gather threat intelligence. This capability enables cybersecurity professionals to stay ahead of emerging threats and understand the tactics employed by cyber adversaries.

Challenges and Ethical Considerations

While the integration of AI in cybersecurity brings immense benefits, it also presents some challenges and ethical considerations that need to be addressed.

Adversarial AI

Cyber attackers have been exploring the concept of adversarial AI, where they use AI-based techniques to craft attacks specifically designed to deceive AI-powered security systems. These attacks exploit the vulnerabilities in the AI algorithms to circumvent detection and infiltrate networks. As AI in cybersecurity evolves, efforts to identify and counter adversarial AI must keep pace.

Data Privacy and Bias

Al relies heavily on data to make accurate decisions. However, the use of vast amounts of data raises concerns

AT ITS CORE, AI IS ABOUT EMPOWERING MACHINES TO LEARN FROM EXPERIENCE, IDENTIFY → PATTERNS, AND MAKE INTELLIGENT DECISIONS WITHOUT EXPLICIT PROGRAMMING.



ADVANCEMENTS IN AI TECHNOLOGIES, INCLUDING QUANTUM COMPUTING AND FEDERATED LEARNING, PROMISE EVEN MORE POTENT DEFENSIVE CAPABILITIES. about user privacy and the potential for perpetuating biases present in the data. Striking a balance between utilizing data for AI models and preserving privacy is a critical challenge for the cybersecurity community.

Human Oversight and Accountability

While AI can automate many cybersecurity tasks, it cannot completely replace human expertise and judgment. Human oversight is crucial to interpret AI-generated insights, address false positives, and ensure ethical decisionmaking in complex scenarios.

The Future of AI in Cybersecurity

As the cyber threat landscape continues to evolve, so will the role of

IN THE DIGITAL AGE, THE PARTNERSHIP BETWEEN ARTIFICIAL INTELLIGENCE AND CYBERSECURITY HAS EMERGED AS THE FRONTLINE DEFENSE AGAINST CYBER THREATS.

Al in cybersecurity. Advancements in Al technologies, including quantum computing and federated learning, promise even more potent defensive capabilities.

With quantum computing, AI can solve complex cryptographic problems more efficiently, enabling robust encryption methods that thwart cyber adversaries. Federated learning allows AI models to be trained collaboratively across multiple organizations without sharing sensitive data, resulting in more comprehensive and diverse threat intelligence.

Additionally, AI-driven security orchestration and automation will streamline incident response processes, enabling cybersecurity teams to focus on strategic decision-making and threat hunting.

In the digital age, the partnership between Artificial Intelligence and Cybersecurity has emerged as the frontline defense against cyber threats. Al's ability to process vast amounts of data, identify anomalies, and adapt to evolving attack vectors provides a formidable shield for safeguarding our digital world.

However, it is essential to recognize that AI is not a panacea; it must be integrated thoughtfully with human expertise, ethical considerations, and proactive measures to stay ahead of cybercriminals. By embracing the potential of AI and nurturing it responsibly, we can ensure a more secure and resilient digital future.

VEEAM PARTNERS WITH MICROSOFT TO BRING NEW DATA PROTECTION AND RANSOMWARE RECOVERY CAPABILITIES TO VEEAM BACKUP FOR MICROSOFT 365

eeam Software, the leader in Data Protection and Ransomware Recovery, has announced it is integrating Veeam Backup for Microsoft 365 with newly launched Microsoft 365 Backup via their backup APIs to bring customers and partners new capabilities for backup, recovery, ransomware protection and business continuity. Veeam plans to utilize this integration to deliver new innovations and experiences to Microsoft customers that need the very best data protection and ransomware recovery to keep their businesses running.

"Today, every business is a digital

business," said Danny Allan, CTO at Veeam. "That means fast, reliable access and availability of data is critical to keep businesses running. Veeam is the leading provider of backup and recovery for Microsoft 365, with over 15 million users protected. We're delighted to extend our advanced capabilities to customers and partners using Microsoft 365 Backup. We plan to deliver innovative new features and capabilities taking advantage of the power and reliability of the Veeam Data Platform which keeps businesses running."

"We're excited to work with Veeam, and look forward to the unprecedented speed and scale of backup and restore



experiences they can bring to customers with our new Microsoft 365 Backup solution," said Jeff Teper, President, Collaboration Apps and Platforms, Microsoft.

Veeam Backup for Microsoft 365

Today, Veeam Backup for Microsoft 365 is the leader in Microsoft 365 backup and is being used to protect more than 15 million users. This adoption reflects customers' shared responsibility to own and protect their critical Microsoft 365 data, eliminating the risk of losing Microsoft 365 data, including Microsoft Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams, Veeam Backup for Microsoft 365 provides the lowest recovery point objectives (RPO), the broadest set of recovery options, and the flexibility to back up Microsoft 365 data to any location. The addition of support for Microsoft 365 Backup will expand those industryleading capabilities and will be available to all Veeam Backup for Microsoft 365 customers when it's available.

For more information about Veeam Backup for Microsoft 365, visit https:// www.veeam.com/backup-microsoftoffice-365.html.

Availability

Work on the integration between Veeam Backup for Microsoft 365 and Microsoft 365 Backup via their backup APIs is underway, with general availability of our updated offering expected within 90 days of the Microsoft 365 Backup service being available. VEEAM BACKUP FOR MICROSOFT 365, WHICH TODAY PROTECTS OVER 15 MILLION MICROSOFT 365 USERS, WILL DELIVER NEW BACKUP AND RESTORE CAPABILITIES WITH MICROSOFT 365 BACKUP

83% OF SUCCESSFUL CYBERATTACKS IN ME HAD A TARGETED NATURE: POSITIVE TECHNOLOGIES

ccording to Positive Technologies' cybersecurity threatscape report, Middle Eastern government entities are especially appealing targets to cybercriminals: 22% of total attacks on organisations targeted government agencies, and 56% of these were perpetrated by APT groups. Armed with various malware and exploits, malicious actors penetrate the victims' networks and linger to conduct cyber espionage.

Industrial companies feel the pressure of cyberattacks, with 16% of companies being threatened, as they possess valuable information, represent components of critical infrastructure, and make a significant contribution to the regional economy. Malicious actors often use social engineering to gain access to victims' systems (33% of cases), and the tools most frequently used in attacks on this sector are remote access trojans (RATs, 62%) and data-wiping malware (31%).

According to analysts, 78% of cyberattacks on organisations in the Middle East target computers, servers, and network equipment. Threat actors compromise systems by deploying malware or exploiting vulnerabilities to steal confidential information or to disrupt the operation of devices.

Malware is critical in cyberattacks on institutions: it was utilised in 58% of attacks on organisations and 70% of attacks on individuals. RATs, which enable attackers to assume control over a compromised device, are the most widely used type of malware. Additionally, spyware, often masquerading as legitimate applications, is extensively used against individuals.

Attacks in the Middle East are notable for the use of wipers, which delete files on compromised devices. Wipers are extremely dangerous when penetrating industrial control systems (ICS), as this can disrupt production processes and lead to accidents.

Experts are particularly concerned about the increasing activity of ransomware groups, which have turned into one of the biggest threats. In Q1 2023, the number of ransomware incidents in the world increased by 77% year-on-year. The most prominent victims of ransomware in the Middle East are GCC countries including the UAE, Saudi Arabia, and Kuwait.

Fedor Chunizhekov, Information Security Analyst at Positive

Technologies, says: "According to our data, 83% of successful cyberattacks in the Middle East countries have a targeted nature. A majority of attacks in the Middle East rely on social engineering, malware, or exploitation of software vulnerabilities. In 2023, the most relevant cybersecurity





threats to the Middle East countries are cyberattacks on government institutions and critical infrastructure, as well as attacks that employ phishing and social engineering techniques. Activities of hacktivists pose a threat as well: their actions can lead to leaks of confidential data, disrupt enterprise operations and even influence important decisions."

Fedor Chunizhekov says this growth in the number of cybercriminal groups and cyberattacks in the Middle East has necessitated increased organizational cybersecurity: according to a forecast by International Data Corporation (IDC), security spending will increase by 8% in 2023, with most (41%) of these funds to be allocated for software. The governments of several countries realise the gravity of these threats and are taking steps to regulate cyberspace. For example, Qatar and Bahrain adopted laws to protect personal data, while the United Arab Emirates established more stringent privacy and data protection standards. These measures are designed to ensure security and raise awareness about the importance of data protection.

Positive Technologies recommends that industrial companies and government institutions take the necessary measures to protect their IT systems, including implementing a comprehensive results-oriented cybersecurity approach aimed at establishing an automated security system that provides uninterrupted protection against non-tolerable events. This approach entails defining and verifying organisation-specific nontolerable events, keeping software up to date, raising employees' cybersecurity awareness, and ensuring constant cyberthreat monitoring and detection by introducing advanced information security tools such as the following:

- Web application firewalls
- SIEM (security information and event management) systems for monitoring and analysis of security events
- XDR (extended detection and response) solutions for timely response
- NTA (network traffic analysis) solutions for deep traffic analysis and detection of malicious activity
- Advanced sandboxes for static and dynamic analysis of threats, including APTs
- VM (vulnerability management) systems for automation of asset management and correctly prioritised detection and remediation of infrastructure vulnerabilities depending on their importance Besides, organisations can use bug bounty platforms to build a continuous service security assessment process and optimise their security spending. 1

WHY ZERO TRUST ARCHITECTURE IS CRITICAL IN SECURING CLOUD-BASED ENTERPRISES

MATT BROMILEY , SANS INSTITUTE

here has been an upsurge in cybercrime in recent years despite widespread commitments to strengthening security posture across the public and private sectors. Global spending on best-ofbreed security solutions and Al-enabled machine learning tools reached record highs in 2022. And even amidst the socioeconomic headwinds of current market conditions, Gartner still forecasts that security and risk management investments are slated to grow by 11% through the end of 2023 – equating to

Despite this, adversarial threat actors continue to seemingly bypass stringent security implementations with ease.

more than \$183.3 billion.

The paradoxical discrepancy is largely rooted in misalignment between common security controls and the evolving cyber threat landscape. With the societal adoption of remote and hybrid work environments following COVID-19, organizations have integrated the use of cloud technologies, services, and third-party applications into functional operations at a rapid scale.

This new way of working expanded the attack surface exponentially, giving adversaries a wider range of external vulnerabilities to target via social engineering campaigns and malwarebased attacks. From the emergence of new business collaboration channels like Slack and Microsoft Teams to the meteoric rise of remote IoT devices, an organization's digital footprint is more exploitable than ever.

Compounding the issue is that many companies have invested in security stacks originally designed to defend complex on-premises environments, not the unstructured data assets of their cloud-based business ecosystems. Given the heightened sophistication and funding of modern cybercrime, organizations must operate under the presumed assumption that their network will be breached — meaning it's not a matter of if, but when.

To align with these changing dynamics, it's critical to shift away from the legacy perimeter-based controls of the past in favor of a more agile zero trust architecture (ZTA) that restricts adversaries from causing irremediable damage after that inevitable breach occurs.

The Building Blocks of ZTA

When approaching the integrated adoption of a successful ZTA model, it's first important to remember that the inherent concept of zero trust extends beyond any single element or control. It's rather a prescribed way of being that weaves security into every layer of the enterprise and guidelines efficient mitigation in the wake of compromise. Removing implicit trust and, in turn, access to specific privileges based on that trust reduces the ability of a compromised account to wreak havoc within the organization's digital ecosystem. Consider it defense indepth.

Achieving a true zero trust environment is not a light switch scenario by any means. ZTA requires a complete architectural overhaul comprised of calculated planning, integration, access/ operations management, and verification mechanisms. It certainly cannot be accomplished with an eye for old practices.

The foundational components of ZTA include identifying/inventorying enterprise assets, determining access policies, establishing where those policies should be implemented, and then controlling how they are maintained. That said, ZTA adoption can only begin with end-to-end visibility into an organization's existing digital infrastructure to identify what assets are of highest value to adversaries. The more attractive the asset, the tighter access policies in place.

For a healthcare system, an example of high-value asset could be sensitive patient medical records containing personally identifiable information. For a financial institution, it could be data logs detailing the third-party vendor transactions and bank account numbers of a large enterprise. For governmental agencies, it could be confidential intelligence relative to matters of public safety. It all depends on the conditions that are unique to the organization's security environment, but regardless of size or sector, they have a responsibility to defend their assets from being leveraged for malicious intent.

Securing the Hybrid Attack Surface

Many enterprises that transitioned from on-premises to hybrid work environments still rely on virtual private networks (VPN) that grant remote users shared access to a myriad of end points and applications. But if a ransomware actor were to steal the right account with the right permissions through an email-borne phishing scheme, that VPN would essentially be rendered useless. After bypassing the narrow perimeter protections, there's nothing stopping them from utilizing the compromised account to encrypt and exfiltrate sensitive data for extortion.

But if that same enterprise had a ZTA model layered within their security environment. access determinations would instead be defined at a centralized Policy Decision Point (PDP) and scaled to the individual user on the principle of least privilege. This time, after the ransomware actor gained access to stolen credentials, a Policy Enforcement Point (PEP) system continuously monitoring the account's activity would already be positioned to identify suspicious behaviors and subsequently terminate the session in real time — thus mitigating the breach's impact. The policies maintained by the PDP/ PEP determine per session what assets each user should and should not access based on certain kev criteria.

In conclusion, it's clear that adversaries have found far too much success attacking today's modern enterprises. Even though we continue to see organizational growth and infrastructure implementations followed by new security tooling and security controls, threat actors continue to find vulnerabilities to capitalize on. These matters are further complicated when we consider the implications of the past 24 to 36 months from a computing and enterprise architecture perspective.

With ZTA adoption, however, all hope is not lost. Organizations with a vast array of resources, systems, applications, and data on a global scale need a security model that can grow at the rate the organization wants to move — not a rate that hinders growth or creates gaps for adversaries to exploit.

SECURITY ANALYSTS IN UAE & KSA FEAR THEY ARE MISSING A RELEVANT SECURITY EVENT: VECTRA AI

WITHOUT VISIBILITY ACROSS THE ENTIRE IT INFRASTRUCTURE, ORGANIZATIONS ARE NOT ABLE TO IDENTIFY EVEN THE MOST COMMON SIGNS OF AN ATTACK.

ectra Al, the pioneer of Aldriven cyber threat detection and response for hybrid and multi-cloud enterprises, has announced the findings of its 2023 State of Threat Detection Research Report, providing insight into the "spiral of more" that is preventing security operations center (SOC) teams from effectively securing their organizations from cyberattacks.

Today's security operations (SecOps) teams are tasked with protecting progressively sophisticated, fast-paced cyberattacks. Yet, the complexity of people, processes, and technology at their disposal is making cyber defense increasingly unsustainable. The everexpanding attack surface combined with evolving attacker methods and increasing SOC analyst workload results in a vicious spiral of more that is preventing security teams from effectively securing their organization. Based on a survey of 2,000 SecOps analysts - including 200 in the UAE and KSA — the report breaks down why the current approach to security operations is not sustainable.

Spiral of More Threatens Regional Security Teams' Ability to Defend Their Organization

Manual alert triage costs organizations \$3.3 billion annually in the US alone,



and security analysts are tasked with the massive undertaking of detecting, investigating and responding to threats as quickly and efficiently as possible while being challenged by an expanding attack surface and thousands of daily security alerts. The study found:

- 48% of IT security analysts in the UAE and KSA report the size of their attack surface has increased in the past three years.
- On average, SOC teams in the UAE and KSA receive 6,736 alerts daily (approx. 2,252 more than the global average) and spend nearly two and a half hours a day manually triaging alerts.
- On average, security analysts in the UAE and KSA are unable to deal with 73% of the daily alerts received, with 85% reporting that alerts are false positives and not worth their time.

SOC Analysts across the UAE and KSA Don't Have the Tools to Do Their Jobs Effectively

Despite a majority of SOC analysts across the UAE and KSA reporting their tools are effective, the combination of blind spots and a high volume of false positive alerts are preventing regional enterprises and their SOC teams from successfully containing cyber risk. Without visibility across the entire IT infrastructure, organizations are not able to identify even the most common signs of an attack, including lateral movement, privilege escalation, and cloud attack hijacking. The study also found:

- 96% of surveyed UAE and KSA SOC analysts worry about missing a relevant security event because it's buried under a flood of alerts. Yet, the vast majority deem their tools effective overall.
- 40% of UAE and KSA security analysts believe alert overload is the norm because vendors are afraid of not flagging an event that could turn out to be important.
- 43% claim that security tools are purchased as a box-ticking exercise to meet compliance requirements,



and 54% wish IT team members consulted them before investing in new products.

UAE and KSA Security Analysts Facing Burnout, Posing Significant Risk to Organizational Security

Despite the increasing adoption of AI and automation tools, the regional security industry still requires a significant number of workers to interpret data, launch investigations, and take remedial action based on the intelligence they are fed. Faced with alert overload and repetitive, mundane tasks, almost three-quarters of security analysts in the UAE and KSA report they are considering or actively leaving their jobs, a statistic that poses a potentially devastating long-term impact to the regional security industry. The study found:

- Despite 73% of UAE and KSA respondents claiming their job matches expectations, 74% are considering leaving or are actively leaving their job.
- Of the analysts considering leaving or actively leaving their role, 31% of surveyed security analysts in the UAE and KSA say it is because they spend

all their time sifting through poor quality security alerts.

• 48% of regional analysts claim they're so busy that they feel like they're doing the work of multiple people, and 44% believe working in the security sector is not a viable long-term career option.

"As enterprises shift to hybrid and multi-cloud environments, security teams are continually faced with more — more attack surface, more attacker methods that evade defenses, more noise, more complexity, and more hybrid attacks," said Kevin Kennedy, senior vice president of products at Vectra Al. "The current approach to threat detection is broken, and the findings of this report prove that the surplus of disparate, siloed tools has created too much detection noise for SOC analysts to successfully manage and instead fosters a noisy environment that's ideal for attackers to invade. As an industry, we cannot continue to feed the spiral, and it's time to hold security vendors accountable for the efficacy of their signal. The more effective the threat signal, the more cyber resilient and effective the SOC becomes." 🚦

SPOTLIGHT / MANAGEENGINE

MANAGEENGINE SHIELD 2023: A GAME-CHANGER IN IAM AND IT SECURITY

he ManageEngine Shield 2023 seminar held in the UAE was a groundbreaking event that brought together industry experts, thought leaders, and key stakeholders to discuss the evolving identity and access management, and IT security landscapes.

ManageEngine demonstrates its unparalleled understanding of industry trends and the evolving security landscape. With cloud adoption, ManageEngine recognizes the significance of identities as the fundamental pillars of security, therefore it offers cuttingedge solutions that enable enterprises to embrace an identity-driven approach. These innovative solutions empower organizations to navigate the complexities of identity access and management, ensuring robust security and efficient operations. Shield 2023 provided invaluable insights and solutions to address these pressing concerns, delivering significant value to all participants.

The esteemed Head of Cybersecurity from the UAE Government, H.E. Dr.

Mohamed Al Kuwaiti, delivered an impactful keynote session at Shield 2023. He emphasized ManageEngine's role in both shielding UAE's security and exporting that security to various platforms, highlighting their significant contributions to the cybersecurity landscape. ManageEngine's cutting-edge IAM and IT security solutions showcased at Shield 2023 are driving a paradigm shift in major UAE organizations. The seamless integration of IAM and IT security ensures that user identities remain protected, vulnerabilities are minimized, and the overall operational efficiency is enhanced.

Veronica Martin spoke to Harish Sekar, Head of Business Development at ManageEngine, about the latest trends in Identity and Access Management, how organisations in the UAE are adapting to the increasing complexity of managing identities and the best practices for implementing IAM solutions.

What are some of the latest trends in Identity and Access Management (IAM) that organisations in the UAE should be aware of? Identity access and security were different in the past, but now identity security is the key. User identity and their passwords are crucial, and security is no longer separate from identity. They are both together. How would you go about provisioning a user with perfect access and at the same time how are you going to keep it secure? This is where the ballgame is today.

Identity security has been underrated. People create accounts but they aren't using strong passwords and that's where security comes into picture. People need to ask themselves: am I using secure passwords? Do I have additional protocols in place, such as multi-factor authentication? How safe is my MFA process now that there are MFA fatigue and other attacks that can even compromise an MFA-protected system?

Eventually when we deal with security, it is to give you additional time to fight an attack. There's no one technology that's going to keep you safe forever. It's all about building it together and ensuring that you have enough time to understand the attack and make sure that you don't lose much data. Identity security is the new frontline of defense and needs immediate attention. Administrators should spend a lot of time thinking about how identities must be created, monitored, and when they're gone, how we should wipe all the information without leaving any traces.

How are organisations in the UAE adapting to the increasing complexity of managing identities and access across multiple systems and platforms?

In the UAE, all companies had firewall and all protocols in place at the office before Covid. If you had to touch an organisational device, you had to follow certain protocols and policies. Then Covid happened, people were working from home and anywhere, but they still needed access to those resources and that's where it split. When dealing with security, your firewall policies have to be looked after and you need to give access to people working from home. How could the user access a specific application? There was some leniency that was provided. Not many people even had a VPN, so how could I get access to the firewall?

There were problems dealing with it immediately. Not many organisations were even equipped, and enterprises suffered because they were not prepared as security is a difficult business. If Covid hadn't happened, people would still be taking security very lightly. The major problem with IT security, dealing with the hybrid infrastructure is where to be a bit lenient and to pull strings.

Can you highlight some of the best practices for implementing IAM solutions in the UAE?

First of all, know your resources, how many people are active, inactive or disabled and how many you wipe on a regular basis. If you don't know the answers for this, there are no chances of you improving your identity, access onboarding process and deprovisioning process. In the UAE users can't be deleted. They have to be disabled for a certain amount of time, and then when compliance allows it, they can

IT'S ALL ABOUT BUILDING IT TOGETHER AND ENSURING THAT YOU HAVE ENOUGH TIME TO UNDERSTAND THE ATTACK AND MAKE SURE THAT YOU DON'T LOSE MUCH DATA.

be deleted. In some industries, you can't delete anything. The best practice I would recommend is to use a strong username and password, make them complex, but at the same time, find a way to make sure users remember them. Let them choose it, show them ways to do it and they will get around it. No weak passwords and do multifactor.

Once you do that, just give enough access and keep eyes all over them. When you create a user, your job is not finished. You have to see what the user is doing. You have to improve the service that could potentially go on them because they're the weakest link and when they do something different, you need to know.

User onboarding, modification and deletion are a lot of work. You need to connect all of these systems into a one stop ecosystem where, when an account is created, everything is automated, and the user gets an email or an SMS with their credentials. Then, when they log in, they have to go ahead and reset their own password. If they switch departments deprovisioning comes out. Everything from top to bottom, permissions they had on the domain file, servers and applications should be revolved.

What are the key challenges faced by organisations in the UAE when it comes to implementing effective SIEM (Security Information and Event Management) solutions?

There's a lot of damage control that needs to be done to understand what's happening in the infrastructure. Administrators just can't go and implement a SIEM because they would've either given it to an MSP or it could be another department looking at it. There are many challenges, but for an organisation where an administrator has just joined, the challenge that they might face is first the customisation part. Because no company wants to spend a lot of money for customisation. Additionally, it's not integrated with the existing infrastructure they have and that's the biggest problem.

How can SIEM solutions be integrated with IAM systems to provide a comprehensive security framework?

When an account is created and the user is with the company for years, eventually you have to study the practice, and this is where monitoring comes in, such as what the users are doing, which machine, how much lateral movement is happening, what services or applications they are using. Basically, studying practices about that specific user. It's not only Windows applications, cloud databases and infrastructure. At the time of onboarding, everything can seem simple, but with years, there's a lot that a user could be doing. From the time of onboarding, you need to start doing user session monitoring.

This is before Windows, after it or any other applications that you might have anything in your network. All of them have to work in tandem. An identity access tool, which is creating, modifying, deleting accounts is also providing them an access on the other side. The same is studying user behaviour. When it raises an anomaly that the person is doing, such as copying, deleting or moving files and jumping into 10 machines at one log in.

All of these are signs of an attack that can work with the identity access through walking the permissions, disabling the user and taking actions immediately through security orchestration automation response. That is why SIEM and identity access should work together. Our in-house SIEM and IAM solutions do just that.

KYNDRYL AND VERITAS INTRODUCE NEW SOLUTIONS FOR DATA PROTECTION AND RECOVERY

yndryl, the world's largest IT infrastructure services provider, and Veritas Technologies, the leader in secure multi-cloud data management, unveiled two new services -- Data Protection Risk Assessment with Veritas and Incident Recovery with Veritas. As a key milestone in Kyndryl and Veritas' strategic alliance, these services help enterprises protect and recover their critical data across on-premises, hybrid and multi-cloud environments.

The Data Protection Risk Assessment with Veritas is delivered through the Kyndryl Consult network of technology experts and provides a cyber resilience maturity assessment that analyzes a customer's IT infrastructure and data against industry best practices. Kyndryl combines its cyber resilience framework with Veritas' data management solutions to identify risks, cyber resilience gaps and security vulnerabilities. The flexible deployment model allows Kyndryl experts to customize the assessment for unique requirements, policies and processes from all types of organizations. The offering also provides unified insights across on-premises, hybrid and cloud environments, leveraging unique data points that give customers the visibility and information to better manage and protect their data.

Incident Recovery with Veritas is a fully managed service encompassing backup, disaster recovery and cyber recovery. A key differentiator of the solution is AI-based autonomous data management capabilities that drive intelligent automation, operational agility, efficiency



at scale, and a consistent experience across clouds for rapid recovery in the event of a cyber incident. The solution enables organizations to mitigate risk and high costs of a data breach by leveraging features such as air-gapped protection, immutable storage, anomaly detection and recovery automation.

"While the benefits of digital modernization and moving to the cloud are undeniable, businesses need to plan for the risks," said Kris Lovejoy, Kyndryl Security and Resiliency Global Practice Leader. "Through our partnership, Kyndryl and Veritas bring years of experience in helping some of the world's largest organizations achieve true cyber resiliency. These new co-developed solutions are designed to give our customers a clear view of their current estate, pinpoint areas for strengthening it and then shore up their security posture for the long term."

"With data now widely distributed, a constantly evolving threat landscape and frequent ransomware attacks, the old methods for protecting data have become obsolete," said Mike Walkey, Veritas Senior Vice President of Global Channels and Strategic Alliances. "Kyndryl and Veritas have combined a deep expertise in managing mission-critical IT environments with trusted data protection, recovery and compliance technology to help enterprises assess risks and keep their data secure, resilient and compliant."

Solar Powered Camera

No network cable required

Powered by solar energy, this kit sets up without any electrical wiring.

Easy installation

Easy set up without mechanical equipment-reducing the installation costs and time.

Can withstand bad weather

Prone to extreme weather such as strong wind and rainstorms.



40W



20 Ah

HIKVISIONMENA

O HIKVISIONMENA

4G

in HIKVISION-MENA

HIKVISIONMENA



HIKVISION



Scan to Learn More

DBS-2000-28P 28-Port Nuclias Cloud-Managed Switch



< nuclias

cloud

With **POWERUL SECURITY** features, including SSL, DHCP Server Screening, 802.1x port/MAC-based authentication & Access Control List (ACL), this Cloud switch is a **VERSATILE SOLUTION** for deployments that require easy configuration, without added complexities.



