Security

ADVISOR

MIDDLE EAST

HIGHLIGHTS

SOPHOS ✳

HUAWEI ✳✳

AXIS COMMUNICATIONS ✳

DIGITAL
FORTRESS

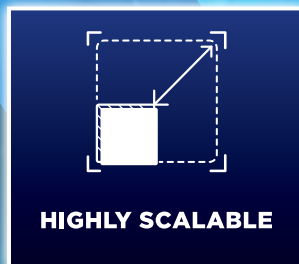**SECURITY ADVISOR MIDDLE EAST TAKES A LOOK AT HOW THE EVOLVING TRENDS IN AI ARE RESHAPING THE CYBERSECURITY LANDSCAPE.**

tahawultech.com

cnme
computer news middle east
SUPPLEMENT

Switching that **Stacks Above the Competition**

Highly Scalable Solutions for a Future-Proof Enterprise Network

HIGHLY SCALABLE

HIGH AVAILABILITY

DXS-F3500-64S

HOT-SWAPPABLE REDUNDANCY

Highlights

Layer 3 10G/40G/100G Managed Switch

VERSATILE MANAGEMENT

Future-proof *your network with 100G uplink port speeds*

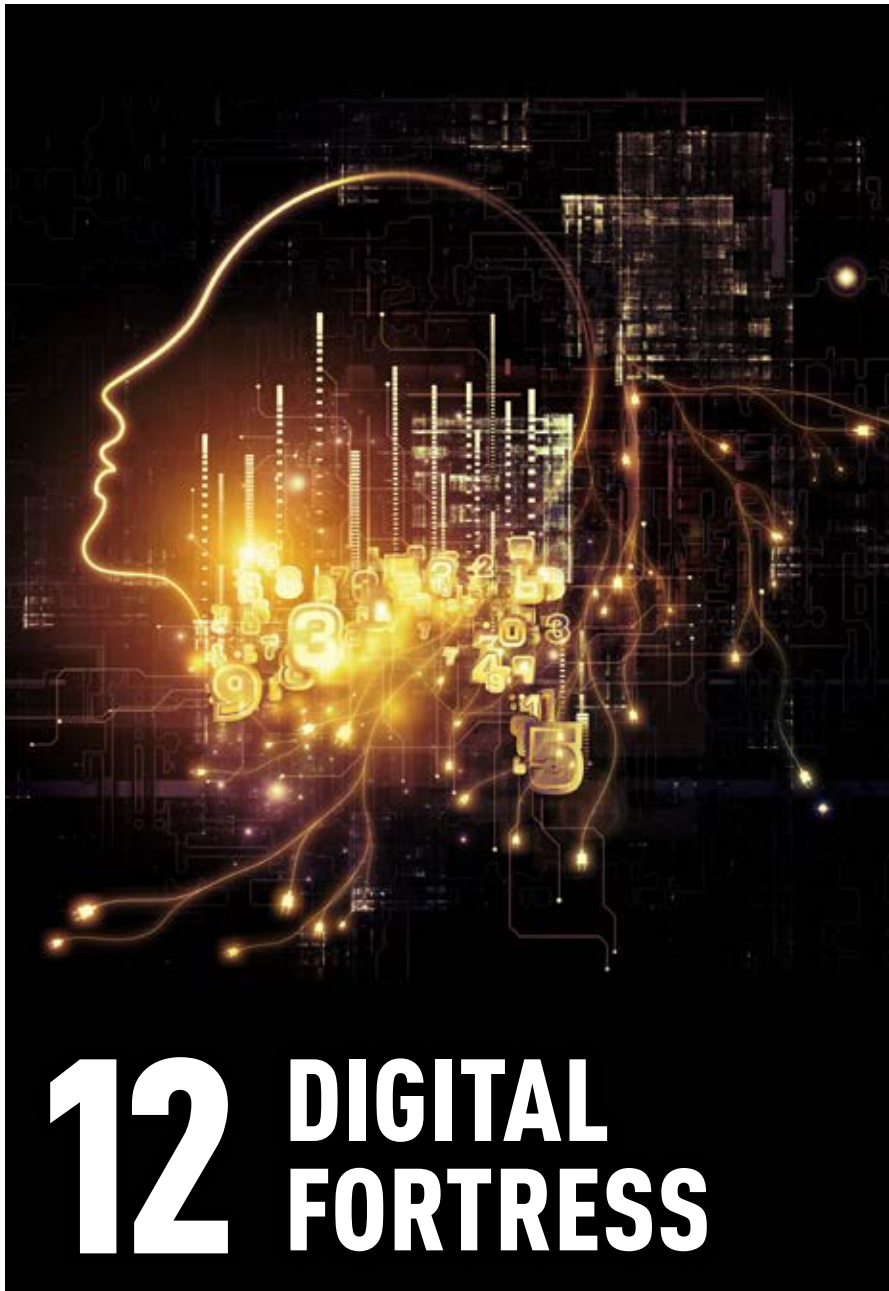**Virtual Switching Unit (VSU) • Enterprise Layer 3 Features**

Advanced Quality of Service (QoS)

D-Link®

Connect to more...

https://me.dlink.com

CONTENTS

16

22

28

12 DIGITAL FORTRESS

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.

2MP @ 30 fps **40**W **20**Ah lithium **4**G Beaufort scale **12** **IP67**

HIKVISION®

EDITOR'S NOTE

THE AGE OF AI

I n an era where technology is the lifeblood of our interconnected world, the battle between malicious actors and defenders of cybersecurity has reached unprecedented heights. As cyber threats grow increasingly sophisticated, the need for advanced and proactive defense mechanisms has become more urgent than ever.

Enter the realm of Artificial Intelligence (AI), where cutting-edge algorithms and machine learning models are revolutionising the field of cybersecurity. From threat detection and prevention to incident response and vulnerability assessments, AI is emerging as a powerful tool in the hands of cyber defenders, enabling them to stay one step ahead in this perpetual cat-and-mouse game.

In this issue, we delve into the fascinating world of AI and its significant impact on cybersecurity. We explore how AI technologies are being leveraged to identify and neutralise threats in real-time, automating tasks that were once painstakingly manual. We examine the role of AI in anomaly detection, behavior analysis, and network security, highlighting its potential to uncover hidden patterns and predict emerging risks before they wreak havoc.

However, as with any technological advancement, there are ethical and privacy concerns that arise alongside the potential benefits. We address these crucial considerations, exploring the delicate balance between security and personal freedoms, as well as the importance of responsible AI development and deployment.

Moreover, we shed light on the collaboration between human experts and AI systems, emphasising the need for a symbiotic relationship that leverages the unique strengths of both to create a formidable defense against cyber threats. The human touch remains essential in interpreting AI-generated insights, making strategic decisions, and addressing the ever-evolving challenges presented by adversaries.

AI TO THE RESCUE

As AI continues to evolve at a rapid pace, it is paramount to stay informed about the latest breakthroughs, innovations, and best practices in the field of cybersecurity. We hope this edition will provide valuable insights into the world of AI and its role in protecting our digital landscapes. Let us embrace the power of AI, while also upholding the values of security, privacy and ethical considerations.

Together, let us embark on a journey into the realm of AI and cybersecurity, and explore the limitless possibilities of this dynamic and critical alliance.

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

Anita Joseph
Editor

EVENTS

tahawultech.com
FUTURE SECURITY AWARDS

tahawultech.com
CISO50
AWARDS & FORUM

KYNDRYL ANNOUNCES CYBERSECURITY INCIDENT RESPONSE AND FORENSICS SERVICE

Kyndryl, the world's largest IT infrastructure services provider, unveiled a Cybersecurity Incident Response and Forensics (CSIRF) service to help customers proactively prepare for and respond to threats by applying the latest threat intelligence and experience from Kyndryl's deep domain security experts. The new service helps customers investigate and respond to a detected security incident by leveraging capabilities such as incident triage, incident response, threat intelligence, compliance monitoring and management. Customers may also select proactive services that may significantly reduce the time to respond to an incident.

Kyndryl's CSIRF service provides integrated and seamless incident response (IR) support, forensics, and recovery capability to help customers analyze, identify, compare, and understand the evidence and causes of a cyber incident. In the event of an occurrence, such as ransomware, Kyndryl's CSIRF experts provide on-demand, hands-on support to assist in resolving threats to a customer's business.

"Cyber resilience is the ability to anticipate, protect against, withstand, and recover from adverse conditions, stresses, attacks, and compromises of cyber-enabled business. CSIRF discovers and responds to detected security incidents and provides advanced threat detection response and forensics," said Kris Lovejoy, Kyndryl Security and Resiliency Global Practice Leader. "Kyndryl's CSIRF is intended to shift the cybersecurity field, from simply security to one of cyber resilience."

The new CSIRF service complements Kyndryl's Recovery Retainer Service, which is designed to help customers recover and rebuild their environments after catastrophic events. When coupled with the Recovery Retainer Service, CSIRF provides on-demand availability of qualified experts that can effectively help customers recover from and mitigate the impact of cyberattacks.

KASPERSKY EDR EXPERT AND KATA NOW DELIVER MORE MANAGEMENT FLEXIBILITY FOR CORPORATE CLIENTS

According to the latest Kaspersky IT Security Economics report, nearly 46% of companies outsource work to external specialists due to the complexity of business processes and infrastructure. In-house staff may not always have the necessary knowledge as the threat landscape is rapidly changing or because they cannot effectively use complex IT security solutions. Keeping this in mind, Kaspersky updates its solutions regularly to adapt them to evolving business and security needs and make working processes easier for customers.

Kaspersky Anti Targeted Attack Platform (KATA) and Kaspersky Endpoint Detection and Response Expert (KEDR Expert) have been updated by allowing to configure Windows operating system settings in a sandbox1 to be more flexible and adaptable to customer's infrastructure. This helps IT Security experts to better distinguish malicious links and files, and makes virtual machines with a fully featured OS more customizable to companies' real business environment. With these new updates clients are able to set up computer and user account names, set system language and install applications.

To enhance the compatibility of Kaspersky Anti Targeted Attack Platform and Kaspersky Endpoint Detection and Response Expert, the EDR agent was integrated into Kaspersky Endpoint Security for Linux and Kaspersky Endpoint Security for Windows. Telemetry collected from this agent can be sent to third-party systems via API providing more efficiency for already existing SIEM, SOAR or XDR systems.

"Our customers have complex infrastructures and need cybersecurity solutions with flexible settings. To meet their needs, we are constantly developing our products, customizing them, and making them easier to manage. By doing this, we are able to contribute to better business cyber resilience," said Veniamin Levtsov, VP, Center of Corporate Business Expertise, Kaspersky.

SECUREWORKS UNIFIES INDUSTRIAL CYBERSECURITY WITH THE FIRST INTEGRATED MDR SOLUTION FOR OT AND IT

Secureworks, a global leader in cybersecurity, has announced two new offerings to unify the way industrial organizations prevent, detect, and respond to threats across the OT and IT landscapes. The convergence of OT and IT in the industrial sector brings technological and economic benefits, but also increases risk. The more OT systems are digitally connected, the larger the overall attack surface becomes, making OT an increasingly attractive target for threat actors. This, combined with a global cybersecurity talent shortage numbering in the millions, has led to unprecedented levels of cyberattacks impacting the industrial sector. According to

Gartner®1, manufacturing companies are now among the most targeted for cyberattacks, comprising 23% of all attacks.

Secureworks Counter Threat Unit data shows that approximately 22% of Secureworks' emergency incident response engagements between April 2022 and April 2023 were in the manufacturing industry alone. Manufacturing made up 20% of all ransomware-based incident response engagements that Secureworks remediated in the same period. Gartner also predicts that by 2025, 70% of asset-intensive organizations will have converged their security functions across both enterprise and operational

environments.2 Yet, in industrial environments overall, OT is often managed differently from IT with no centralized visibility across both.

CLOUDFLARE PARTNERS WITH KNOWBE4 TO EQUIP ORGANIZATIONS WITH REAL-TIME SECURITY COACHING TO AVOID PHISHING ATTACKS

Cloudflare's cloud email security solution, Area 1, now integrates with KnowBe4, a leading security awareness training and simulated phishing platform. This integration allows mutual customers to offer real-time coaching to their employees when a phishing campaign is detected by Cloudflare's email security solution.

Phishing attacks often use email as a vector to deliver the fraudulent message. Cybercriminals use a range of tactics, such as posing as a trustworthy organization, using urgent or threatening language, or creating a sense of urgency to entice the recipient to click on a link or download an attachment.

Despite the increasing sophistication

of these attacks and the solutions to stop them, human error remains the weakest link in this chain of events. This is because humans can be easily manipulated or deceived, especially when they are distracted or rushed. For example, an employee might accidentally

click on a link in an email that looks legitimate but is actually a phishing attempt, or they might enter their password into a fake login page without realizing it. According to the 2021 Verizon Data Breach Investigations Report, phishing was the most common form of social engineering attack, accounting for 36% of all breaches. The report also noted that 85% of all breaches involved a human element, such as human error or social engineering.

Therefore, it is essential to educate and train individuals on how to recognize and avoid phishing attacks. This includes raising awareness of common phishing tactics and training individuals to scrutinize emails carefully before clicking on any links or downloading attachments.

ESET RESEARCH REVEALS NEW ANALYSIS OF ACECRYPTOR: USED BY CRIMEWARE, IT HITS COMPUTERS 10,000 TIMES EVERY MONTH

ESET researchers revealed today details about a prevalent cryptor malware, AceCryptor, which operates as a cryptor-as-a-service used by tens of malware families. This threat has been around since 2016, and has been distributed worldwide, with multiple threat actors actively using it to spread packed malware in their campaigns. During 2021 and 2022, ESET telemetry detected over 240,000 detection hits of this malware, which amounts to over 10,000 hits every month. It is likely sold on dark web or underground forums, and tens of different malware families have used the services of this malware. Many rely on this cryptor as their main protection against static detections.

"For malware authors, protecting their creations against detection is challenging. Cryptors are the first layer of defense for malware that gets distributed. Even though threat actors can create and maintain their own custom cryptors, for crimeware threat actors, it often may be time-consuming or technically difficult to maintain their cryptor in a fully undetectable state. Demand for such protection has created multiple cryptor-as-a-service options that pack malware," says ESET researcher Jakub Kaloč, who analyzed AceCryptor.

Among the malware families found that used AceCryptor, one of the most prevalent was RedLine Stealer – malware available for purchase on underground forums and used to steal credit card credentials and other sensitive data, upload and download files, and even steal cryptocurrency. RedLine Stealer was first seen in Q1 2022; distributors have used AceCryptor since then, and continue to do so. "Thus, being able to reliably detect AceCryptor not only helps us with visibility into new emerging threats, but also with monitoring the activities of threat actors," said Kaloč.

NETSCOUT INTRODUCES MOBILE SECURITY FOR 4G/5G NETWORKS

NETSCOUT SYSTEMS, INC. has introduced Arbor Sightline Mobile and MobileStream to answer mobile network operators' (MNO) need for scalable, real-time visibility, detection, and mitigation of threats that can impact the performance and availability of 4G/5G mobile consumer services and network infrastructure. As the market leader in carrier-grade service assurance solutions, NETSCOUT continues to expand its Visibility Without Borders® platform by combining its best-of-breed mobile network telemetry capabilities with its market-leading DDoS protection technology to provide MNOs with a unique solution to identify and eliminate malicious traffic before it impacts subscribers and the network.

According to recent reports, global mobile data traffic will increase four-fold between 2022 and 2028 to more than 325 exabytes per month, led by the growth in consumer IoT devices, mobile gaming, and the rollout of 5G. Unfortunately, mobile threat activity is expanding in tandem with this traffic growth. NETSCOUT's DDoS Threat Intelligence Report identified a 79% increase in DDoS attacks targeting mobile subscribers from 2020 to 2022. And, with ever-growing numbers of vulnerable consumer devices connected to mobile networks, directly or via fixed wireless access (FWA), many of the same botnet-related problems plaguing wireline networks are now threatening mobile services.

"Mobile network operators are facing new security challenges as they expand their enterprise and consumer broadband offerings," said Patrick Donegan, founder and principal analyst, HardenStance, Ltd. "NETSCOUT is combining its proven Adaptive Service Intelligence (ASI) deep packet inspection and Arbor Sightline threat detection technologies to provide mobile network operators scalable, cost-effective visibility into their customers' mobile core traffic so they can identify and manage threats before they impact their services and reputation."

The new Arbor Sightline Mobile provides MNOs with comprehensive visibility into their mobile traffic to detect and manage cyberthreats in a scalable way not previously available to quickly eliminate mobile subscriber and device disruptions. Arbor Sightline Mobile consumes user and control plane telemetry streamed from NETSCOUT's MobileStream network monitoring instrumentation. MobileStream uses NETSCOUT's patented ASI to extract meta-data from 4G/5G traffic as it traverses the mobile core – enabling user traffic visibility to be correlated with subscriber and device identities for real-time threat detection, attribution, reporting, and analytics at network scale.

WHAT'S EASY TO SEE IN OUR CLOUD? OPPORTUNITY.

It's easier than ever to access advanced cloud analytics with SAS® Viya® on Microsoft Azure. Viya is optimized for Azure, which means it's easier to find, share and analyze information all in one place. So more people can ask the questions that lead to more opportunities. Together, SAS and Microsoft make it easier to find answers in the cloud.

Learn how at sas.com/microsoft

TECHNOLOGY INNOVATION INSTITUTE ANNOUNCES OPEN SOURCE LAUNCH OF UAE'S FIRST LANGUAGE MODEL TRAINED ON AMAZON SAGEMAKER

Amazon Web Services, Inc. (AWS), an Amazon.com, Inc. company, has announced that Technology Innovation Institute (TII), the applied research pillar of Abu Dhabi's Advanced Technology Research Council, trained its top-performing, open source Falcon 40B model on AWS. Falcon 40B is a 40-billion-parameter large language model (LLM) available under the Apache 2.0 license that ranked #1 in Hugging Face's Open LLM Leaderboard, which tracks, ranks, and evaluates LLMs across multiple benchmarks to identify top performing models. It was trained on 1 trillion tokens on Amazon SageMaker, a fully managed service for developing, training, tuning, and hosting machine learning models, including LLMs. The launch represents a significant milestone in the UAE's commitment to fostering AI innovation and scientific contributions in line with the UAE National AI Strategy 2031.

Customers can now deploy Falcon 40B from Amazon SageMaker JumpStart, a machine learning (ML) hub that offers pre-trained models, giving customers access to Falcon 40B's state-of-the-art accuracy and industry-leading performance without having to build their own model from scratch. To get started with Amazon SageMaker JumpStart, visit aws.amazon.com/sagemaker/jumpstart.

Dr. Ebtesam Almazrouei, Executive Director – Acting Chief AI Researcher of AI Cross Center Unit and Project Lead for LLM Projects at TII, highlighted Falcon 40B in a new blogpost, stating: "We proudly announce the official open-source release of Falcon-40B, the world's top-ranking open-source language model. Falcon 40B is an exceptional open-source model with 40B parameters, specifically designed as a causal decoder-only model. It was trained on a vast dataset of 1,000B tokens, including RefinedWeb enhanced with curated corpora. By releasing Falcon-40B as an open-source model, we provide researchers, entrepreneurs, and organizations with the opportunity to harness its exceptional capabilities and drive advancements in AI-driven solutions from healthcare to space, finance, advanced manufacturing to biotech; the possibilities for AI-driven solutions are boundless.

TII announced its Falcon 40B model in March 2023, and released it as an open source in May 2023 under the Apache 2.0 license. Falcon 40B has outperformed contemporary models in multiple benchmarks without fine-tuning. Amazon SageMaker Jumpstart makes Falcon 40B easier for customers to access. Now customers of any size and industry can quickly and easily deploy their own Falcon 40B model and customise it for translation, question answering, summarising information, or identifying images.

With Falcon LLM 40B, organizations worldwide can access its advanced tech capabilities and empower researchers to drive innovation in AI. To learn more about the Falcon LLM 40B model and how it can revolutionize industries, please visit FalconLLM.tii.ae

DIGITAL
FORTRESS

SECURITY ADVISOR MIDDLE EAST TAKES A LOOK AT HOW THE EVOLVING
TRENDS IN AI ARE RESHAPING THE CYBERSECURITY LANDSCAPE.

In an increasingly interconnected and digitized world, the importance of cybersecurity cannot be overstated. As cyber threats become more sophisticated and pervasive, traditional security measures alone are no longer sufficient. This is where Artificial Intelligence (AI) comes into play, revolutionising the field of cybersecurity. By leveraging AI technologies, organisations can enhance their defense mechanisms, identify emerging threats, and respond rapidly to cyber incidents. This article explores the role of AI in cybersecurity, its applications, benefits, challenges, and the future prospects of this powerful alliance.

Artificial Intelligence, with its ability to analyse vast amounts of data, learn patterns, and make intelligent decisions, is transforming the cybersecurity landscape. It enhances security measures by automating processes, augmenting human capabilities, and bolstering threat detection and response capabilities. AI's role in cybersecurity can be categorized into three key areas:

Threat Detection: AI algorithms can analyze large volumes of data to identify patterns, anomalies, and indicators of compromise that might be missed by traditional security tools. Machine learning models can recognize known attack signatures and adapt to evolving threats through continuous learning. This enables proactive threat detection and prevention, reducing response time and minimizing potential damage.

Incident Response: AI-powered security systems can autonomously respond to cyber incidents by isolating affected systems, mitigating risks, and initiating appropriate remediation actions. This helps in containing the impact of attacks and reducing the burden on human responders. AI can also provide real-time alerts and recommendations to security analysts, enabling quicker and more effective decision-making.

Vulnerability Management: AI can assist in identifying vulnerabilities in networks, systems, and applications. It can perform automated scans, analyze security configurations, and assess potential weaknesses. By prioritizing vulnerabilities based on their severity and potential impact, AI helps organizations allocate their resources effectively for remediation efforts.

Applications of Artificial Intelligence in Cybersecurity: AI finds its applications across various domains within cybersecurity, strengthening defenses and safeguarding critical assets. Here are some key areas where AI is making a significant impact:

1. Malware Detection: Traditional signature-based antivirus solutions struggle to keep up with the ever-evolving malware landscape. AI-powered malware detection systems employ behavior-based analysis, anomaly detection, and machine learning techniques to detect and combat known and unknown malware threats.

2. User and Entity Behavior Analytics (UEBA): AI algorithms can analyse user behavior, network traffic, and system logs to establish baseline patterns and detect anomalies indicative of insider threats, account compromise, or unauthorized access attempts. UEBA helps in early detection of suspicious activities and potential breaches.

3. Network Security: AI-enabled network security solutions monitor network traffic, identify potential intrusions, and detect suspicious activities in real-time. By employing machine learning and deep learning algorithms, these systems can identify emerging threats, anomalous traffic patterns, and potential zero-day attacks.

ARTIFICIAL INTELLIGENCE, WITH ITS ABILITY TO ANALYSE VAST AMOUNTS OF DATA, LEARN PATTERNS, AND MAKE INTELLIGENT DECISIONS, IS TRANSFORMING THE CYBERSECURITY LANDSCAPE.

4. Phishing and Fraud Detection: AI-powered algorithms can analyze email contents, URLs, and sender reputations to identify phishing attempts and fraudulent activities. Natural language processing (NLP) techniques enable the detection of social engineering tactics and the classification of suspicious emails.

5. Security Analytics and Threat Intelligence: AI-driven security analytics platforms combine data from various sources, such as threat intelligence feeds, logs, and external indicators, to provide comprehensive insights into security posture. Machine learning algorithms help identify correlations, uncover hidden patterns, and generate actionable intelligence.

6. Predictive Analytics: By analyzing historical security data, AI algorithms can predict future attack vectors, vulnerabilities, and potential breach scenarios. This allows organizations to proactively strengthen their defenses, prioritize security measures, and allocate resources effectively.

Benefits and Challenges of AI in Cybersecurity: The adoption of AI in cybersecurity brings numerous benefits, but it also presents certain challenges that need to be addressed. Let's examine the advantages and the associated concerns:

Benefits of AI in Cybersecurity: a. Enhanced Threat Detection: AI algorithms can quickly and accurately detect threats, even in large and complex datasets, improving the overall security posture. b. Reduced Response Time: Automated incident response and real-time alerts enable organizations to respond swiftly

> **BY ANALYSING HISTORICAL SECURITY DATA, AI ALGORITHMS CAN PREDICT FUTURE ATTACK VECTORS, VULNERABILITIES, AND POTENTIAL BREACH SCENARIOS.**

to cyber threats, minimizing potential damages. c. Scalability and Efficiency: AI systems can handle vast amounts of data and perform complex analysis at a speed unattainable by humans, allowing organizations to scale their cybersecurity efforts. d. Augmented Decision-making: AI provides security analysts with actionable insights, enabling them to make informed decisions and prioritize response efforts effectively. e. Adaptability to Evolving Threats: Machine learning models can continuously learn from new data, adapting to emerging threats and staying ahead of attackers.

Challenges of AI in Cybersecurity: a. Adversarial Attacks: AI models themselves can be targeted and manipulated by adversaries, leading to potential vulnerabilities and false negatives. b. Lack of Transparency: Complex AI algorithms can be challenging to interpret, making it difficult to understand the rationale behind decisions and potentially hindering trust. c. Data Quality and Bias: AI relies heavily on data, and if the training data is incomplete, biased, or of poor quality, it can lead to inaccurate

predictions and false positives/negatives. d. Privacy and Ethical Concerns: The use of AI in cybersecurity raises privacy concerns, particularly when analyzing user behavior and personal data. Ethical considerations regarding data usage and potential biases also need to be addressed.

The future of AI in cybersecurity looks promising, with ongoing advancements and research. Here are some key areas of development and future prospects:

1. Explainable AI: Efforts are underway to develop AI systems that can provide clear explanations for their decisions, increasing transparency and enabling better trust and accountability.
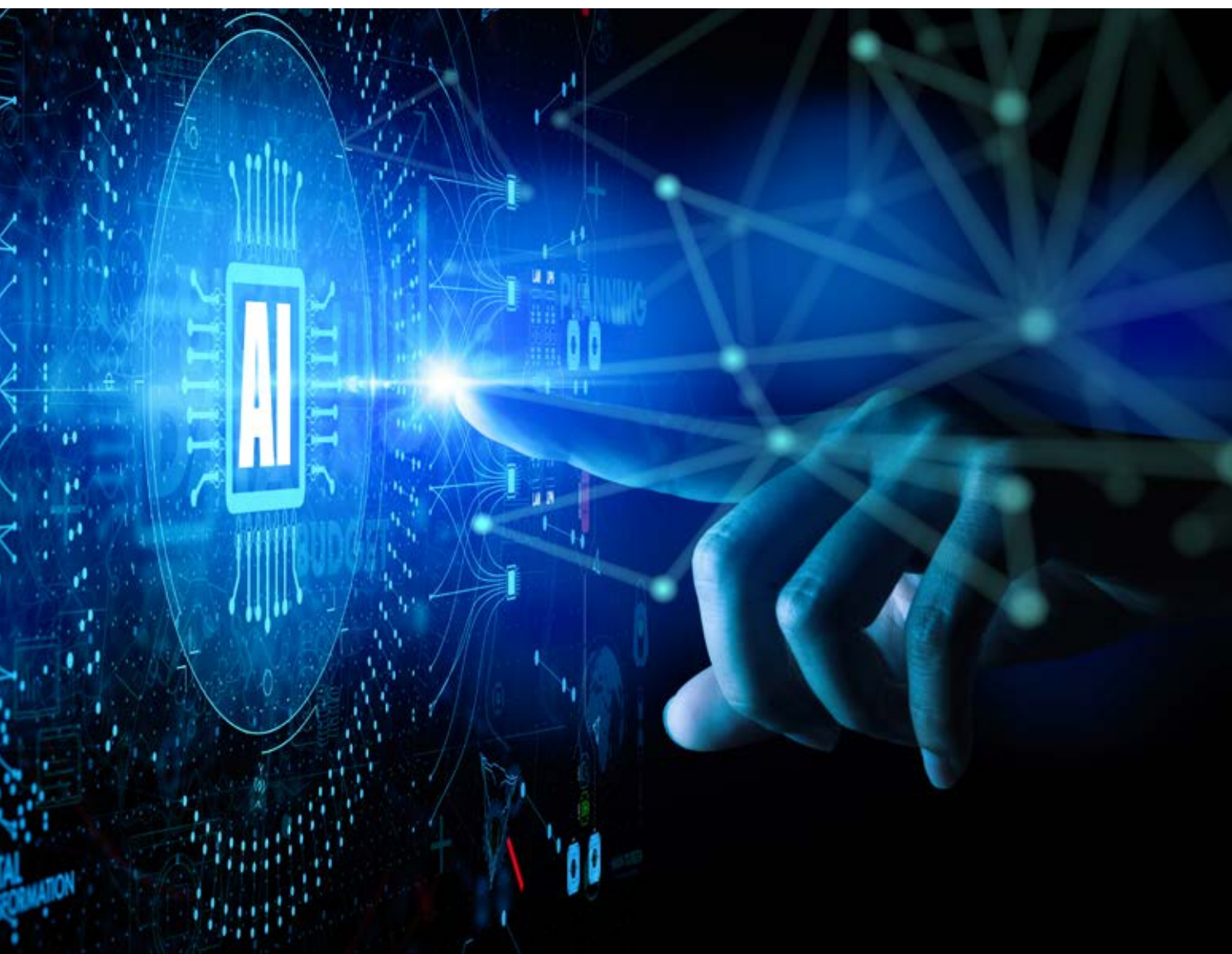
> **AI-POWERED SECURITY SYSTEMS CAN AUTONOMOUSLY RESPOND TO CYBER INCIDENTS BY ISOLATING AFFECTED SYSTEMS, MITIGATING RISKS AND INITIATING APPROPRIATE REMEDIATION ACTIONS.**

2. **AI and Big Data Analytics Integration:** The integration of AI with big data analytics will enable organizations to harness the power of vast amounts of data for more accurate threat detection, predictive analytics, and actionable insights.

3. **Zero Trust and AI:** AI technologies will play a vital role in implementing zero trust architectures by continuously monitoring and analyzing user behavior, network traffic and access requests.

4. **AI-Enabled Autonomous Systems:** The development of AI-driven autonomous systems will automate routine security tasks, respond to threats in real-time, and enable human security experts to focus on more strategic activities.

In conclusion, the fusion of Artificial Intelligence and cybersecurity is revolutionizing the way organizations defend against cyber threats. AI's ability to analyze vast amounts of data, detect anomalies, and adapt to evolving threats empowers organizations to bolster their defense mechanisms, enhance incident response capabilities, and proactively mitigate risks. While challenges such as adversarial attacks and transparency need to be addressed, the future prospects of AI in cybersecurity are promising. As technology evolves, it is essential to strike a balance between innovation, security, and ethical considerations to harness the full potential of AI for a safer digital landscape. ▪

AI MODELS THEMSELVES CAN BE TARGETED AND MANIPULATED BY ADVERSARIES, LEADING TO POTENTIAL VULNERABILITIES AND FALSE NEGATIVES.

PROTECTING ASSETS IN A REMOTE-FIRST (AND POTENTIALLY HOSTILE) WORLD

WITH BOTH PERSISTENT ATTACKS AND POST-PANDEMIC REMOTE WORK HERE TO STAY, MODERN SECURITY SOLUTIONS MUST ASSUME THE ENDPOINT DEVICE OR PHONE OPERATES IN A DANGEROUS ENVIRONMENT AT ALL TIMES SAYS **CHESTER WISNIEWSKI**, FIELD CTO, SOPHOS

I live in the city center and the lunch hour certainly isn't like it once was. While some people have returned to working in an office, it seems that the majority have not. Looking back, the pandemic will have been a turning point for many things around the world, and the rhythms of office-centered work life will be something that will never return to the old ways.

With this increased flexibility employees are not just working from home behind consumer-grade Wi-Fi routers; they are also spending part of the day at the park or coffee shop, or perhaps even having a "working holiday." Those in charge of protecting enterprise assets have to assume these endpoints are always in hostile territory.

Even before the pandemic, organizations working toward improving their security maturity were often trying to "push left." What is pushing left? At its most basic level it means moving things closer to the start. It originates from software development where the stages of the development process are conceptualized from left to right, left being the beginning. In applied security we also use the term "pushing left," but rather than referring to the software development process we are referring to the attack chain, which moves

from reconnaissance on the left through action (exfiltration or other attacker goal) on the right.

For many years, the most comprehensive security strategies have involved defense in depth. The idea is that not all technologies are suitable for detecting a given threat type, so it is best to deploy them in layers. These layers often directly correspond to how far "left" something is in the attack chain. If you can detect something at the network border through your firewall, email, or web filters, you have contained the threat before it has any negative impact on operations.

Ideally you want to detect and block an attacker as far left as possible, i.e., as early as possible. Pushing detections left also alerts security analysts that an intrusion may be underway, initiating more focused threat hunting to anticipate gaps in defenses your attacker may be attempting to exploit.

For employees at the office, you can centralize control of these defenses and provide optimum protection. The question is, are you able to provide the same protection for remote workers regardless of their location? Can you monitor and respond to threats being detected on

those assets when they are out of the office? As many have observed, this did not work as well as we would have liked when we all went into lockdown, many of us without a plan.

While there are still many benefits to monitoring the network when you have control of it, including reduced endpoint overhead and the ability to keep threats at a distance from sensitive assets, we need to ensure we can take as much of this protection as possible with us when we are out and about.

We must ensure not only that protection is optimized, but also that we don't lose our ability to monitor, detect, and respond to attacks targeting these remote assets. Most organizations have moved to utilizing EDR/XDR solutions (or plan to in the very near future) , which is a great start, but not all solutions are comprehensive.

In the remote-work era, insufficiently protected remote users can encounter plenty of issues – malicious URLs and downloads, and networks attacks, to name only the most mundane – that in the Before Times would have been handled by machines guarding the corporate "fort." The biggest missing components when users are "outside the fort" are HTTPS

filtering and web content inspection of the sort that is typically implemented within next-generation firewalls. When you add these technologies to pre-execution protection, behavioral detection, machine learning models, client firewalls, DLP, application control, and XDR, you are starting to look at a comprehensive stack of defenses for attackers to overcome – even if the endpoints themselves are now free-range.

For initiatives like zero trust network access (ZTNA) to be effective, we must not only wrap the applications we interact with, but we must also wrap the endpoints that connect to them. Simple checks like whether the OS up-to-date and whether it has security software installed may be a good start, but not all protection is created equal.

With most devices being connected to the internet whenever they're in use, we can leverage the power of the cloud to help provide ubiquitous protection and monitoring. Modern security solutions must assume the endpoint device or phone is in a hostile environment at all times. The old idea of inside and outside is not only outdated, it's downright dangerous. ♟

BUILDING
TRUST WITH AI

ALOYSIUS CHEANG, CHIEF SECURITY OFFICER, HUAWEI MIDDLE EAST AND CENTRAL ASIA, TELLS ANITA JOSEPH HOW THE COMPANY AIMS TO LEVERAGE THE GROWING DEMAND FOR AI TO AUTOMATE DEFENCE AND ATTACK CAPABILITIES.

The threat-security landscape has been continuously evolving and growing. What is your take on this?

The pandemic has accelerated the demand for digital transformation, to support remote work arrangements. Many resources that were previously located in offices have now become standard at home. As we transition out of the pandemic era, organizations are looking to improve their operations and expand into new territories, especially those with regional focus. They want to explore how they can better support their businesses and adopt technologies like AI.

In recent months, there has been a lot of discussion about generative AI, such as GPT-based chat systems, and the potential benefits they offer. However, before venturing into any new technology, it is crucial to consider different perspectives, conduct risk assessments, and ensure a thorough approach. The demand for new technologies like AI is skyrocketing, surpassing even the pace set by the pandemic-driven digital transformation. With these emerging technologies, such as generative AI and interactive systems, it becomes essential to reassess strategies and implementation models. Wholesale adoption without careful consideration can lead to risks and challenges, much like navigating a pandemic.

When it comes to AI, one aspect to consider is how to build trust and resiliency in AI systems. This topic has gained attention from AI thought leaders who emphasize the need for careful consideration. It is essential to address ethical issues and have a well-thought-out plan. Although there might not be comprehensive AI laws and regulations in place yet, it is important to be aware of the potential risks. Misuse of AI can lead to reputational damage, financial losses, privacy breaches, and even threats to life. For instance, generative AI could be exploited for cyberbullying or impersonation in financial transactions where voice prints are used for authentication.

Therefore, trust and resiliency should be at the core of any strategy or adoption plan for new technologies, including AI, as part of digital transformation efforts. Cybersecurity needs to be prioritized right from the beginning, rather than as an afterthought or a reactive measure. It is crucial to ensure that cybersecurity is integrated into the design and implementation process, and not treated as a separate add-on.

How does Huawei incorporate security into its operations and product fabric?

Cybersecurity has undergone significant evolution over the past 10 to 15 years. In 2012, we released our first white paper, focusing primarily on cybersecurity and addressing governance, risk, and compliance (GRC) concerns. As we expanded into new markets, we encountered numerous laws and regulations that varied from region to region. Consequently, our cybersecurity position paper emphasized the localization of laws and compliance requirements specific to each market.

Fast forward to 2018, when we issued our second cybersecurity position paper. In this master plan, we transitioned from a GRC-centric approach to an end-to-end cybersecurity assurance system.

We integrated cybersecurity into every aspect of our organization, considering people, processes, and technology as vital components. Our strategy, which was established in 2011, identified cybersecurity as our top priority. By 2018, we had further reinforced this priority, ensuring that a cybersecurity mindset was ingrained in every individual and process within the company. We implemented training and equitation processes for cybersecurity personnel, emphasizing the importance of security in all our activities.

Our product development lifecycle incorporated the ABC theory—assume nothing, believe no one, and check everything—we implemented a supply chain aggregation process requiring security accreditation for every vendor, local or international. Our focus shifted beyond mere defence to viewing cybersecurity as a weapon of mass destruction, considering the potential impact on critical infrastructure and national security. We developed an end-to-end secure supply chain using our comprehensive security assurance systems, encompassing people, processes, and technology.

With the advent of AI, we are currently working on our cybersecurity 3.0 master plan. We aim to leverage AI for automated defence and attack capabilities. Proactive defence is our primary goal, aligning cybersecurity closely with our company's business strategy. Our objective is to establish cybersecurity as a competitive advantage and a critical business enabler.

This ongoing evolution in cybersecurity demonstrates our commitment to staying ahead of emerging threats and harnessing new technologies to safeguard our organization and provide a competitive edge.

What are the most significant threats currently faced by corporations or businesses in the region? In other words, what is the primary challenge they are confronting?

The primary challenge lies in the people factor. In this region, there is a shortage of skilled cybersecurity professionals, which poses a significant hurdle for businesses. Furthermore, the end users of technology often lack proper security awareness programs, leading to basic mistakes like clicking on malicious links or falling for phishing scams. Even individuals in the cybersecurity field can be susceptible to such threats due to their realistic nature.

To address this challenge, it is crucial to prioritize people awareness training. By educating users about cybersecurity best practices, we can minimize the risks associated with human error. Additionally, closing the cybersecurity manpower gap is a key objective. We aim to provide individuals with a foundational understanding of cybersecurity, enabling them to not only recognize the potential risks posed by emerging technologies like cloud computing, AI, and IoT but also leverage them to gain competitive advantage in their business operations.

It is essential to shift the perception of cybersecurity from being perceived as a mere disruption to a valued asset. By helping people see the inherent value of cybersecurity, we can overcome the cowboy mentality that views it as an obstacle hindering daily tasks and instead recognize it as an essential safeguard for achieving objectives and ensuring business continuity. 🏃

Transforming Network Data into Real Insights

GET THE INSIGHTS, CONTEXT, AND CONTROL YOU NEED WITH POWERFUL FEATURES LIKE:

Incident analytics
- ML-driven root cause analysis and remediation
- AI-driven severity classification

Network health monitoring
- Create and monitor SLA categories and thresholds

Client troubleshooting
- Granular client connection diagnostics and event correlation

Data Explorer
- Customizable visualization of historical data

Reporting
- Curated reports of historical data

Service validation
- Network self-validation via virtual client that resides on RUCKUS access point

Melissa AI-powered virtual network assistant
- Answers IT questions in natural language

IT service management integrations
- Integration via webhooks with leading ITSM platforms such as ServiceNow and Salesforce to automatically initiate helpdesk tickets

Designate a third party for management
- Two-tiered management—log in once to access multiple customer accounts under management

RUCKUS Analytics is a next-generation service for network analytics and assurance. Powered by machine learning (ML) and artificial intelligence (AI), it delivers comprehensive visibility into the operation of your RUCKUS enterprise network. The service accelerates troubleshooting and helps IT teams meet their network SLAs. With streaming network telemetry from network devices, RUCKUS Analytics automatically transforms data into deep insight. Get the information you need to be much more efficient in network assurance—freeing up time to focus on other projects. RUCKUS Analytics supports SmartZone and RUCKUS Cloud control and management architectures. If you prefer, you can designate a third party such as a RUCKUS networking solution provider to administer your account. Managed service providers (MSPs) can manage multiple end-customer RUCKUS Analytics accounts from within their own account.

Want to learn more? Scan this QR code and book a demo!

12 TIPS TO KEEP YOUR BUSINESS SAFE FROM CYBERATTACKS

MOHAMAD RIZK, REGIONAL DIRECTOR, MIDDLE EAST & CIS AT VEEAM SOFTWARE

According to recent research, more than 85% of companies have been the victim of a ransomware attack in the past year. It's not a question of whether you've been attacked or when you'll be attacked, but how often you'll be attacked. While there is no way to guarantee you will never be attacked, you can take some simple steps to make it more difficult for the attackers to succeed and keep your business running. Start with the basics. Make sure your PCs and servers are all up to date and patched. Make sure you have up-to-date virus and malware checks in place. Then, embrace good practices and educate others across your team.

Tip #1 - Be skeptical
If something sounds too good to be true, it probably is. Know the warning signs for phishing, social engineering and other scams and err on the side of caution. Don't click on unknown links, open unexpected or suspicious attachments or provide information to someone you don't know or weren't expecting to hear from.

Tip #2 - Use Strong Passwords and Passphrases
Longer is stronger. Leverage passphrases to help create long passwords that are easy to remember, but hard for others to guess.

Tip #3 - Slow down
Slow down and avoid making simple mistakes. Be cautious of auto-completion in emails so you don't send sensitive information to the wrong person. Don't accidentally 'reply all' when you only intended to send information to one person on the thread.

Tip #4 - Beware of Malware
Viruses, computer worms and Trojans can hide in legitimate looking websites, free software packages online and phishing emails. Ensure you have an anti-malware program enabled and kept updated.

Tip #5 - Stay Secure on the Go
Security doesn't stop just when you leave the office. Be aware of your surroundings. Don't talk about sensitive information, like banking details or medical information, in a location where others can hear you. Keep your device screens hard for others to see - consider a privacy screen when possible. Use an external battery pack rather than public charging ports to protect against 'juice jacking.'

Tip #6 - Know Your Data. Protect It.
You cannot protect your most sensitive information if you don't know what information you have. Inventory your organization's information. Classify it based on its sensitivity level. Protect the information according to that sensitivity level.

Tip #7 - Limit Access
You may hire the most trustworthy people to work for you, but that doesn't mean they all need access to your most sensitive information. Provide access on a need-to-know basis. This helps protect confidentiality, but also reduces the impact if someone's access is compromised. Use multi-factor

authentication when given the option to minimize the damage that can be caused if someone steals your passwords.

Tip #8 - Stay Secure Online

If you understand that the internet contains scams and threats around most corners, then you can help to spot when something doesn't seem right and steer clear. Use and require secure networks - if the WiFi you are using is not encrypted, ensure you are using a VPN or other layer of protection. Leverage bookmarks for important URLs so you're less likely to fall for fake dupes of the real ones. Avoid oversharing on social media and assume that anything posted is public, regardless of privacy settings.

Tip #9 - Be Security Aware. Report.

Even with all the best intentions, sometimes the cyber criminals will win a battle. It is important that your organization has a defined incident reporting and response plan, so that your security team is promptly notified if there is the risk of compromise. The sooner your team knows about it, the sooner they can protect against it. Communicate your preferred method of incident reporting frequently so your employees have no doubt about how to contact you.

Tip #10 - If You Can Connect It, Protect It.

As the perimeter of your business infrastructure becomes blurred with cloud services and personal devices being used for work (BYOD), you need to ensure your corporate policies are inclusive to require that any device used for work that can connect to the internet is required to be protected. This may be anti-malware software, strong passwords or access controls. Each device will require something different, but a general rule of thumb is that if you can connect it, protect it.

Tip #11 – Back up Your Data

You can have a best-in-class security program and still find yourself in a situation where your data can no longer be accessed or trusted. Regularly backing up your data in 3 different locations on 2 different media with 1 copy being offsite, 1 copy being offline, air-gapped or immutable and 0 errors with recovery verification (Veeam's 3-2-1-1-0 rule), allows you to quickly restore your data with minimal downtime and keep your business running.

Tip #12 - Train Your Users // Be a Security Learner

Cyber criminals are constantly changing their tactics as they learn about what protections are being put in place. Your organization's people can either be your weakest link or your greatest asset. Put emphasis in teaching your people about how they can be part of your human firewall, and they can become an extension of your security team. ♟

رقميـــات
Raqmiyat

Secure Your Digital Future

Simple. Secure. Resilient.

Secure Your Enterprise IT Footprint For A Safer Digital Journey

www.raqmiyat.com

UAE | KSA | INDIA

SECURITY IS A SHARED RESPONSIBILITY

ANITA JOSEPH CAUGHT UP WITH **STEVEN KENNY**, ARCHITECT AND ENGINEERING PROGRAM MANAGER – EMEA AT AXIS COMMUNICATIONS TO FIND OUT MORE ABOUT THEIR RECENT SECURITY EVENT, CONNECT AND HOW THE COMPANY COMBINES INTELLIGENT TECHNOLOGY WITH HUMAN IMAGINATION, TO IMAGINE THE NEEDS OF TOMORROW.

Tell us about your event's focus in AUH?
The purpose of the event is to highlight strategically important areas to Axis that are well aligned to various initiatives that will influence the direction of the UAE market. Topics such as Cybersecurity and Sustainability are global challenges that need to be addressed across the UAE and events like Connect will help to build awareness around these issues and what all organizations can do to safeguard themselves, their customers and support government initiatives

What aspects of cybersecurity are you discussing?
The cybersecurity session at the connect events has the purpose of building awareness of the cybersecurity threats association with physical and electronic security systems. The very systems that have been provided to protect an organizations, people, assets etc, may become a cybersecurity risk if not designed, installed and maintained correctly.

The connect events will discuss and highlight research carried out to support the growing threats of a cyberattacks, offer examples where physical security systems have been attacked, the cause of the breach and the business impact. We will also highlight the mitigation factors that will reduce the risk of a business become the next target. Cybersecurity is a shared responsibility across all stakeholders. We will demonstrate the importance of each stakeholder and why supply chain due diligence should be a mandatory requirement.

Do you have any numbers to share on the cybersecurity threats in the region?
The UAE is no different to many other regions across the globe when we consider the threats related to cybersecurity, as the attacks are borderless. The interconnected nature of the internet and digital networks allows cyber threats to transcend geographical boundaries. Cybercriminals can launch attacks from anywhere in the world, targeting individuals, organizations, and even governments across international borders. Whilst the cybersecurity landscape continues to evolve, this makes it difficult to maintain accurate statistics, however the UAE's Telecommunications Regulatory Authority (TRA) reported a significant increase in cyber incidents, with a 250% surge compared to the previous year.

The risk will continue to increase due to the ongoing investment across the region, especially when we consider the increased focus on digital transformation initiatives. Whilst digital transformation brings numerous benefits, it also introduces new vulnerabilities and risks that can be exploited by cybercriminals. Organisations need to ask themselves if they are adequately prepared.

Whilst business continue to face challenges around Phishing Attacks, Ransomware attacks, they need to be mindful of the impact of the insider threat and possible threats of social engineering. For the purposes of the Connect event, organisations need to evaluate their supply chain partners and the increase risk that this will introduce to their business. IoT / OT vulnerabilities are on the rise, as are Advanced Persistent Threats (APTs) which are sophisticated attacks with the purpose of gaining unauthorised access to sensitive information.

What are Axis's plans for the coming months

Axis will continue to work with partners and educate on the importance of cybersecurity. The process will not only build the awareness of the ongoing challenges of a cyberattack, but also what is needed to mitigate the risk of Axis solutions being the cause of an attack. With continued investment in cybersecurity measures, such as commissioning and maintenance tools, product features etc, we endeavor to work with our partners and end clients to make sure the benefit from this continued investment.

THE INTERCONNECTED NATURE OF THE INTERNET AND DIGITAL NETWORKS ALLOWS CYBER THREATS TO TRANSCEND GEOGRAPHICAL BOUNDARIES.

LEGITIMATE ANDROID APP IRECORDER TURNS MALICIOUS WITHIN A YEAR, SPIES ON ITS USERS: **ESET**

THE MALICIOUS APP IS CAPABLE OF RECORDING AUDIO USING THE DEVICE'S MICROPHONE AND STEALING FILES.

ESET researchers have discovered a trojanized Android app named iRecorder - Screen Recorder. It was available on Google Play as a legitimate app in September 2021, with malicious functionality most likely added in August 2022. During its existence, the app was installed on more than 50,000 devices. The malicious code that was added to the clean version of iRecorder is based on the open-source AhMyth Android RAT (remote access trojan)

and has been customized into what ESET named AhRat. The malicious app is capable of recording audio using the device's microphone and stealing files, suggesting it might be part of an espionage campaign.

Besides the Google Play Store, ESET Research has not detected AhRat anywhere else in the wild. However, this is not the first time that AhMyth-based Android malware has been available on the official store; ESET previously published research on such a trojanized app in 2019. Back then, the spyware, built on the foundations of AhMyth, circumvented Google's app-vetting process twice, as a malicious app providing radio streaming. However, the iRecorder app can also be found on alternative and unofficial Android markets, and the developer also provides other applications on Google Play, but they don't contain malicious code.

"The AhRat research case serves as a good example of how an initially legitimate application can transform into a malicious one, even after many months, spying on its users and compromising their privacy. While it is possible that the app developer had intended to build up a user base before compromising their Android devices through an update or that a malicious actor introduced this change in the app; so far, we have no evidence for either of these hypotheses," explains ESET researcher Lukáš Štefanko, who discovered and investigated the threat.

The remotely controlled AhRat is

a customization of the open-source AhMyth RAT, which means that the authors of the malicious app invested significant effort into understanding the code of both the app and the back end, ultimately adapting it to suit their own needs.
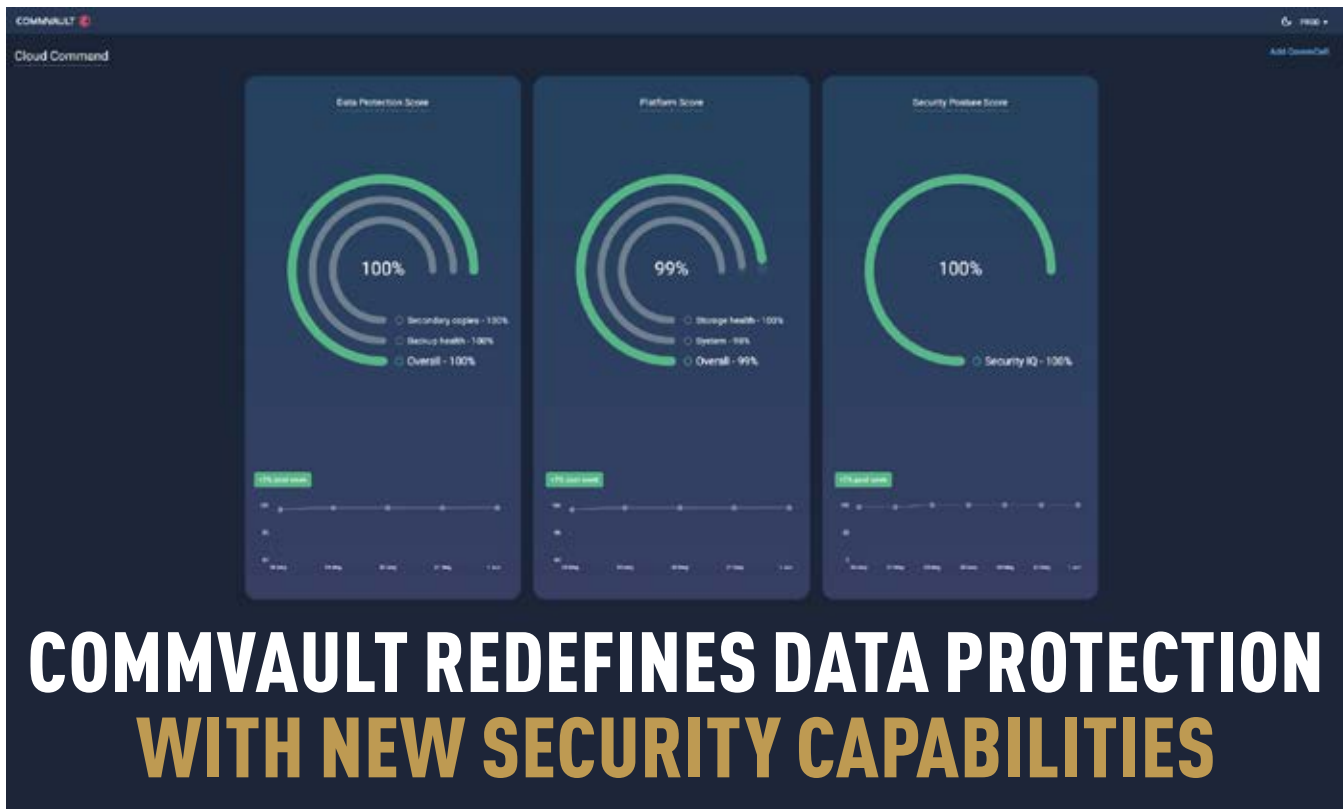
Aside from providing legitimate screen recording functionality, the malicious iRecorder can record surrounding audio from the device's microphone and upload it to the attacker's command and control server. It can also exfiltrate from the device files with extensions representing saved web pages, images, audio, video, and document files, and file formats used for compressing multiple files.

Android users who installed an earlier version of iRecorder (prior to version 1.3.8), which lacked any malicious features, would have unknowingly exposed their devices to AhRat if they subsequently updated the app either manually or automatically, even without granting any further app permission approval.

"Fortunately, preventive measures against such malicious actions have already been implemented in Android 11 and higher versions in the form of app hibernation. This feature effectively places apps that have been dormant for several months into a hibernation state, thereby resetting their runtime permissions and preventing malicious apps from functioning as intended. The malicious app was removed from Google Play after our alert, which confirms that the need for protection to be provided through multiple layers, such as ESET Mobile Security, remains essential for safeguarding devices against potential security breaches," concludes Štefanko.

ESET Research has not yet found any concrete evidence that would enable the attribution of this activity to a particular campaign or APT group. ⚲

COMMVAULT REDEFINES DATA PROTECTION
WITH NEW SECURITY CAPABILITIES

Commvault, an enterprise data protection leader for today's global businesses and the first data protection vendor to introduce cyber deception, announced new security capabilities across its entire portfolio. Signaling the next phase in its evolution, Commvault is helping businesses secure, defend, and recover their data to meet increasingly sophisticated cyberthreats head on. As part of these capabilities, Commvault has expanded its security ecosystem to include product integrations with Microsoft and CyberArk.

Commvault has redefined data protection to include early warning technologies that help to secure against threats before they happen, defend enterprise data if the environment is breached, and ensure recoverability so customers and their data remain resilient in the face of evolving cyber threats. The only data protection vendor with early warning, in-depth threat monitoring, and cyber deception for production and backup environments, Commvault can detect threats in as little as five minutes versus the industry average of 24 hours. Through early detection of zero-day and

insider threats, Commvault technology helps protect data against breaches and cyber-attacks.

Available in Q2, Commvault's advanced security features are managed and delivered through the simplicity of the new Commvault Cloud Command interface, providing complete visibility for better business decisions, improved security postures, and preserved data for cleaner, more efficient recoverability.

"Commvault has spent the last four years redefining and expanding the capabilities of our platform to bridge the gap between IT and security. As a result, our customers can now be on the offense, taking it to the attackers by consolidating threat defense, backup, and recovery in a way that's never been done before," said Sanjay Mirchandani, CEO, Commvault.

"Today we advance on our vision of enhanced data protection that establishes a seamless relationship between threat events and backups – resulting in a rapid and reliable solution for data recovery in the event of a cyber incident," said Rajiv Kottomtharayil, Chief Product Officer, Commvault.

In the event that enterprises need to recover from an attack or outage,

Commvault's proactive and reliable recoverability across the industry's broadest workload coverage reduces downtime and accelerates response times for business continuity.

"We love the simplicity of the Commvault dashboard. With just a few clicks, we can restore a virtual machine or backups after an attack which is vital in our line of work as a pharmaceutical company with very sensitive data," said Paul Vries, IT Consultant, Bilthoven Biologicals. "Commvault gives us confidence that we can manage, protect, and recover data in the cloud and on-premises, even in the worst-case scenario."

Commvault also announced collaborations with Microsoft and CyberArk to integrate Commvault's technology with their respective security platforms. By expanding its security ecosystem, Commvault is helping organizations enhance their security posture through automated incident response, better collaboration, and deeper insights into the threat landscape.

Commvault's latest security innovations will be available in Q2 through Commvault and its worldwide ecosystem of partners. ♟

TryMe™
Scan to experience

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.

ring
an amazon company

For more information, contact mea@ring.com or visit www.ring.com

UAE & KSA IT SECURITY DECISION MAKERS THINK ROLE OF CYBERSECURITY IN BUSINESS SUCCESS OVERLOOKED: DELINEA

DISCONNECT BETWEEN SECURITY AND BUSINESS GOALS HAD NEGATIVE CONSEQUENCES FOR 94% OF RESPONDENTS AND INCREASED THE SUCCESS OF CYBER-ATTACKS AT ONE IN FOUR COMPANIES

Delinea, a leading provider of solutions that seamlessly extend Privileged Access Management (PAM), has announced findings from a global survey of IT Security Decision Makers (ITSDMs) from across the globe – including the UAE and Saudi Arabia - revealing the impact of misalignment between the cybersecurity function and wider business.

Asked about the Board and C-Suite's understanding of cybersecurity across the organization, only 37% of respondents in the UAE and Saudi Arabia think their company's leadership has a sound understanding of cybersecurity's role as a business enabler. Over a third (34%) of respondents believe that it is considered important only in terms of compliance and regulatory demands, while one in five said it is not seen as a business priority. Furthermore, just over half of respondents (55%) believe that there is a "strong alignment" between business and cybersecurity objectives.

The disconnect appears to have caused at least one negative consequence to 94% of regional respondents' organizations, with more than a quarter (28%) also reporting it resulted in an increased number of successful cyber-attacks at their company.

The impact of misaligned goals on the cybersecurity posture of organisations in the UAE and Saudi Arabia was wide-

ranging as it contributed to delays in investments (42%), delays in strategic decision making (41%), and unnecessary increases in spending (33%).

Metrics and processes don't focus on business outcomes

Structural processes are key to aligning goals and, encouragingly, the survey revealed that over two thirds of security teams (68%) meet regularly with their business counterparts at the highest level. Additionally, the majority 62% of companies in the UAE and Saudi Arabia have also embedded security team members within business functions. However, the research showed there is still room to improve, as half of organisations are not documenting policies and procedures to facilitate alignment, and a further 39% reported that alignment is ad hoc and only 'happens when needed.'

The report also brought to light that metrics used to measure and demonstrate the value that cybersecurity delivers. Interestingly, improved experience for business users (33%) was cited as the most important measure of success, followed by more technical and activity-based metrics such as meeting compliance objectives (32%) and reducing costs of security incidents (29%).

"While security teams appear to be more ingrained into the organisational processes, it is clear that the majority of regional enterprises still fail to consider cybersecurity as a competitive advantage," said Mohammad Ismail, Regional Director – Middle East, Delinea. "What's more concerning is that our report shows that this disconnection translates into delayed investments, which put the business at risk, It is time for company leaders to reassess their approach to cybersecurity – seeing it as not just as an obligation, but as a profit center."

"Cyber security can be a huge business enabler, but this research reflects that there is still some work to do at the board level in shifting mindsets. Executive leaders need to think of cybersecurity not only in terms of ticking the compliance box or protecting the company, but also in terms of the value it can deliver at a more strategic level," said Joseph Carson, Chief Security Scientist and Advisory CISO at Delinea.

Making the business case to the board: gaps in ITSDM skillsets and changing lines of reporting

Building out business skillsets may provide the path to better alignment, however respondents in the UAE and Saudi Arabia listed technical skills as the most valuable for cybersecurity leaders to possess. These are rated above skills such as communication, collaboration, business acumen, and managing people.

Aligning goals also involves reviewing the reporting lines and CEO-level visibility. However, the Delinea survey suggests that there is little appetite for change in reporting structures, as less than a third (31%) of regional ITSDMs believe the CISOs or the most senior cybersecurity leaders should report to the CEO to best align cybersecurity with the overall goals of the business.

"Alignment between cybersecurity and business goals is essential for success. This research clearly highlights the negative consequences when teams' objectives aren't fully in sync. Ensuring common agreement across business functions is vital and there is a real value in metrics that not only measure security activity, but which also demonstrate the impact on business outcomes," Carson added. "Communication is key, and while strong technical skills are still important, security leaders need the ability to communicate, influence and present the value they add to business outcomes more frequently than ever. Security leaders that demonstrate this mix of skills, and that have the same end goal in sight as the business, are a force to be reckoned with."

THE REPORT ALSO BROUGHT TO LIGHT THAT METRICS USED TO MEASURE AND DEMONSTRATE THE VALUE THAT CYBERSECURITY DELIVERS.

ALMOST $30K STOLEN VIA FAKE HARDWARE WALLET: KASPERSKY

Cryptocurrency investors often turn to hardware wallets as a secure way to store their digital assets, assuming that they are impenetrable. However, even the most advanced hardware wallets on the market may not be foolproof, and there are still risks associated with using fake or infected devices. Kaspersky shared the details behind the incident of cryptocurrency theft involving a hardware wallet, which resulted in the loss of 1.33 BTC worth $29,585.

Hardware wallets, also known as 'cold' wallets, store cryptocurrency keys on a device the size of a USB stick, which must be plugged into a computer to send crypto or interact with decentralized finance protocols. As a result, these devices are generally considered safer than 'hot' wallets that are connected to the internet at all times.

However, a recent investigation by Kaspersky revealed a rare case of theft of assets from a hardware wallet, demonstrating how cybercriminals are

coming up with new tactics to maximize their profits. The victim did not make any transactions that day, and the cold wallet was not connected to the computer. Thus, the victim did not immediately notice the theft, and the fraudster transferred 1.33 BTC (worth around $29,585) without the victim's knowledge.

Although the copy we studied appeared identical to the original, the device showed signs of malicious tampering upon opening it. Rather than being welded together ultrasonically like genuine hardware wallets, each half of the device was filled with glue and held together with double-sided tape. Additionally, the wallet had a different microcontroller with read protection mechanisms and the flash memory completely disabled, instead of the original one. This led company's researchers to conclude that the victim had purchased a hardware wallet that had already been infected.

The attackers made only three changes to the original firmware of the bootloader and the wallet itself. They removed the

control of protective mechanisms, replaced the randomly generated seed phrase with one of the 20 preset phrases, and used only the first character of any additional password. This gave the attackers a total of 1280 options to pick the key per one wallet.

'Hardware wallets have long been considered one of the safest ways to store cryptocurrency, but cybercriminals have found new ways to benefit by selling infected or fake devices to unsuspecting victims. Such attacks are totally preventable. Hence, we strongly advise users to only purchase hardware wallets from official and trusted sources to minimize the risk," said Stanislav Golovanov, Cyber Incidents Investigation Expert.

To keep crypto assets safe, Kaspersky experts recommend:

- Purchase from official sources: Only buy hardware wallets from official and trusted sources, such as the manufacturer's website or authorized resellers.
- Check for signs of tampering: Before using a new hardware wallet, inspect it for any signs of tampering, such as scratches, glue, or mismatched components.
- Verify the firmware: Always verify that the firmware on the hardware wallet is legitimate and up-to-date. This can be done by checking the manufacturer's website for the latest version.
- Secure your seed phrase: When setting up your hardware wallet, make sure to write down and securely store your seed phrase. A reliable security solution, such as Kaspersky Premium, will protect your crypto details stored on your mobile or PC.
- Use a strong password: If your hardware wallet allows for a password, use a strong and unique one. Avoid using easily guessable passwords or reusing passwords from other accounts. ☥
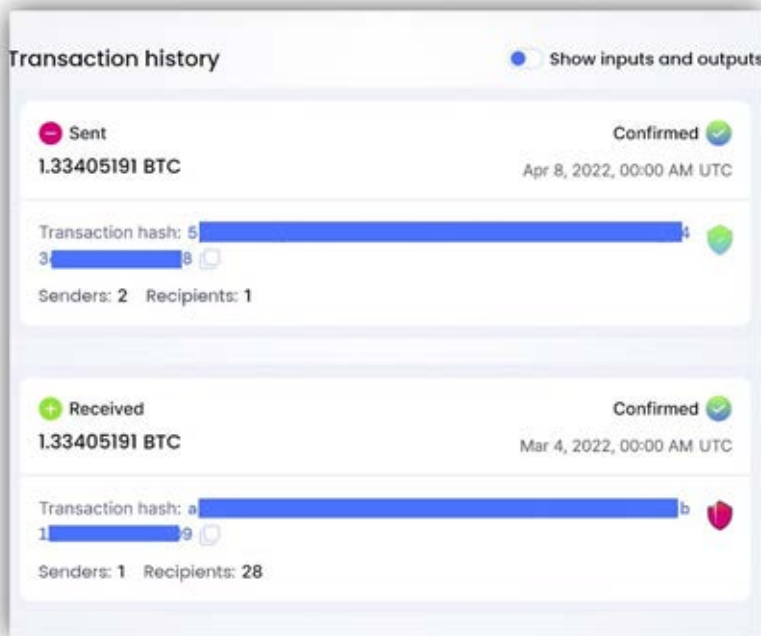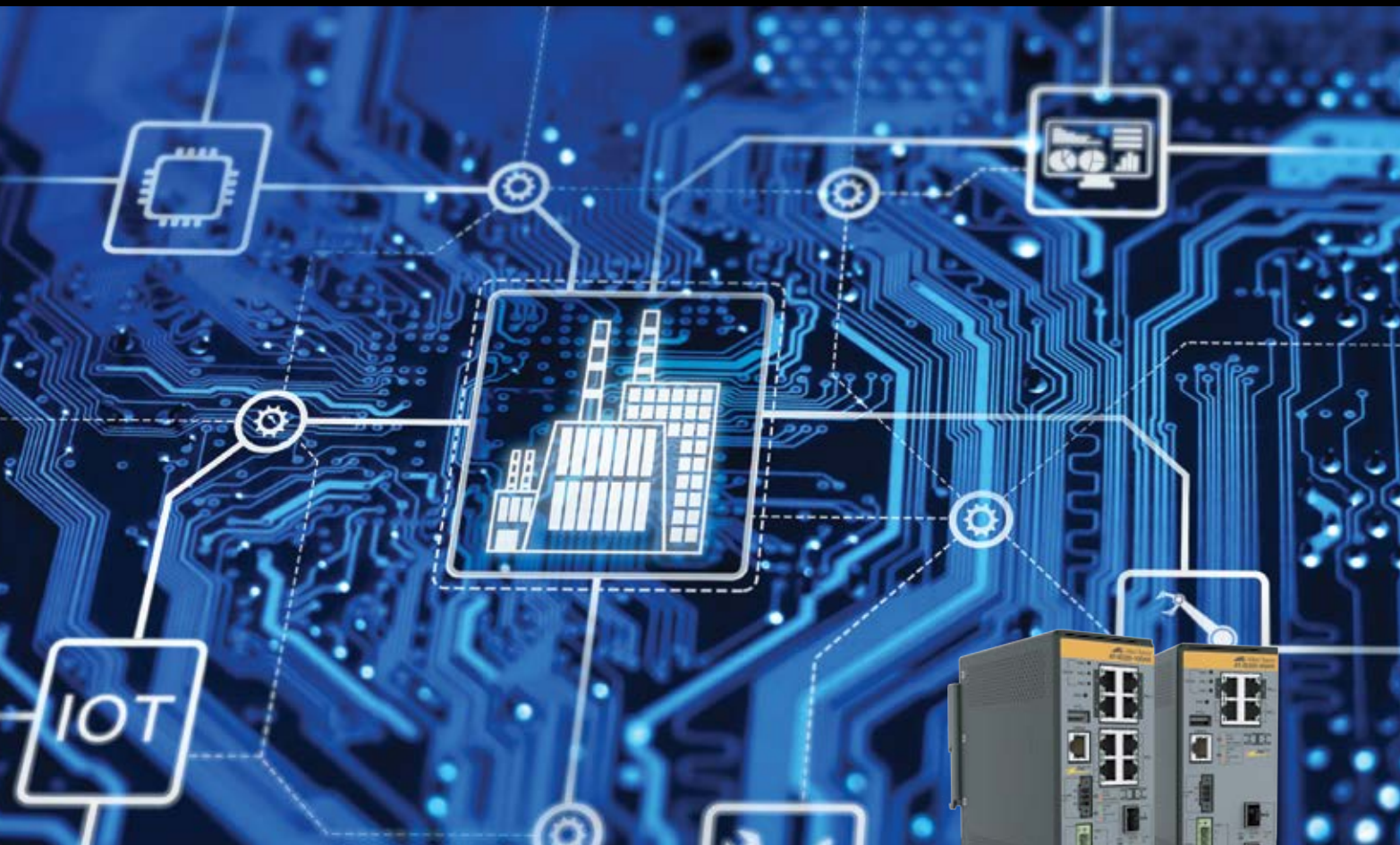
COMMVAULT®

Be data ready.

Commvault is a worldwide leader in delivering data readiness. Our intelligent data management solutions work on-prem and in the cloud, allowing you to store, protect, optimize, and use your data. Always.

commvault.com