ADVISOR

MIDDLE EAST

A

ISSUE 79 | NOVEMBER 2023

HIGHLIGHTS

AFRICAN-EASTERN 🔷

- SYNOLOGY 🔶
- POSITIVE TECHNOLOGIES 🔷

SECURITY IN THE DIGITAL AGE

A

1

1

SECURITY ADVISOR MIDDLE EAST TAKES A NEXT-GENERATION APPROACH TO CYBERSECURITY AND ANALYSES THE VARIOUS THREATS, TRENDS AND DEFENCE MECHANISMS AT PLAY.







Contact Us:

- 🕓 +971 4 801 2222
- reach@morohub.com
- www.morohub.com

Information is Power

Protect it with Moro Hub Cybersecurity Services



Moro Hub offers the best-in-class cyber security services that provides 360-degree protection, delivered from its state-of-the-art Cyber Defense Centre to ensure cyber resilience of your organization's infrastructure.



Identity Intelligence Centre for IAM



WAEE Security Awareness Platform



-

Secure Extended Detection and Response (XDR)

Compliance (GRC) Services

Governance, Risk and



OT & IoT Security Services



Cyber Exposure Services

CONTENTS







18



6 News from the cybersecurity industry in the region and beyond

18 Spencer Pitts of VMWare on the Zero Trust approach to security.

22 Santosh John Thomas, CIO at African-Eastern, on the company's cybersecurity journey and its partnership with Secureworks for cutting-edge SOC services.

28 Michael Chang, Regional Manager at Synology Inc, on how the company is redefining data management with its cutting-edge products and solutions. security capabilities.

Get Started with AQUILA PRO AI App





- Filtra

0 1



AQUILA PRO AI

AQUILAPROAI Wi-Fi Designed To Meet The Needs of The Smart Home

M60

Mesh Your Way to Perfect Wi-Fi 6

Ideal for simultaneous 8K streaming, gaming, and video calls



Fast, Reliable Wi-Fi Connectivity

Ideal for building a solid Wi Fi 6 home network

D-Link[®]



D-Liss

Extend Your Wi-Fi with Ease

Ideal for extending the coverage of your existing Wi-Fi network



EDITOR'S NOTE



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

> Anita Joseph Editor

EVENTS



NAVIGATING THE NEXUS: ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

n the digital age, where the pulse of society beats in binary code, the symbiotic relationship between Artificial Intelligence (AI) and cybersecurity is more pivotal than ever. As we witness unprecedented technological advancements, the stakes of protecting our digital infrastructure against malicious actors have reached new heights. AI emerges as both a formidable ally and a potential double-edged sword in the realm of cybersecurity.

On the positive front, Al brings a transformative paradigm shift to cybersecurity, enhancing our ability

to detect and respond

to threats with unprecedented speed and precision. Machine learning algorithms analyse vast datasets, identifying patterns and anomalies that human analysts might overlook. This proactive approach allows for the swift identification of potential vulnerabilities, enabling preemptive actions to fortify digital defenses. Al-driven threat intelligence also empowers organisations to stay ahead of the curve, adapting to evolving cyber threats in real-time.

However, the power of AI in the hands of malevolent actors poses an equal, if not

greater, risk. As cybercriminals leverage AI to create sophisticated attacks, the cat-and-mouse game between defenders and perpetrators escalates. Deepfakes, automated phishing campaigns, and AIdriven social engineering attacks blur the lines between authentic and manipulated information, challenging the very foundations of trust in our interconnected world.

Navigating this delicate balance requires a multi-faceted approach. Policymakers must foster international collaboration

REAL-TIME THREAT INTELLIGENCE to establish ethical frameworks governing the use of AI in cybersecurity. The development of

standardised protocols and regulations can ensure that AI technologies serve the collective interest while mitigating potential risks. Simultaneously, investment in AI education and training programs is paramount to cultivating a workforce equipped to harness the full potential of these technologies responsibly.

As we stand at the crossroads of innovation and security, a harmonious integration of AI into our defence strategies is the key to safeguarding the digital realm for generations to come.

FOUNDER, CPI Dominic De Sousa (1959-2015)

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

Online Editor

Daniel Shenherd

PRODUCTION AND DESIGN Designer Prajith Payyapilly prajith.payyapilly@cpimediagroup.com DIGITAL SERVICES Web Developer Adarsh Snehajan webmaster@cpimediagroup.com Publication licensed by Dubai Production City, DCCA PO Box 13700

Dubai, UAE Tel: +971 4 5682993

© Copyright 2023 CPI 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.

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

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

Contributing Editor SAME & Tahawultech Veronica Martin



SOLARWINDS BOLSTERS DATABASE OBSERVABILITY FOR CLOUD-NATIVE PLATFORM

SolarWinds, a leading provider of

simple, powerful, secure observability and IT management software, has announced major enhancements to its Database Observability capability within the cloudbased SolarWinds Observability platform. SolarWinds Database Observability provides full visibility into open-source, cloud-enabled, and NoSQL databases to identify and address costly and critical threats to their systems and business.

Database Observability is part of the SolarWinds Database Performance Management portfolio, which includes SQL Sentry and Database Performance Analyzer. With the new capabilities, SolarWinds now offers one of the most comprehen Manageme Database to the succ strategy. Howeve to son chall face busi to-d precis observ struggle root cause risking cos quality of s

comprehensive Database Performance Management portfolios in the industry. Database performance is critical to the success of an organization's IT strategy and business operations. However, databases also lead to some of the most complex challenges that IT teams face due to the complicated, business-critical, and difficultto-diagnose issues they often present. Without complete and precise database monitoring and observability, IT and DevOps teams struggle to accurately diagnose the root cause of performance issuesrisking costly downtime, decreased quality of service delivery, and other critical threats to health and growth potential of the entire enterprise.

VEEAM ANNOUNCES UPDATES TO BACKUP FOR SALESFORCE ON SALESFORCE APPEXCHANGE

Veeam Software, the leader in

Data Protection and Ransomware Recovery, has launched Veeam Backup for Salesforce v2, available on Salesforce AppExchange Veeam Backup for Salesforce eliminates the risks of Salesforce data and metadata loss from human, integration, and corruption errors. This newest version from Veeam — the #1 data protection provider — extends support for multiple clouds, provides greater security with single sign-on (SSO) and multifactor authentication (MFA). and provides a safe environment for testing and developing via sandbox seeding. Organizations can deploy on-premises or in the cloud, recover exactly what they need when they need it, and experience backup that is custom-engineered for Salesforce data and metadata.

Data loss is inevitable within an organization, so it's important for organizations to protect themselves at all costs. This newest version builds on the success of Veeam Backup for Salesforce with its already powerful, rapid-recovery capabilities for IT departments and Salesforce administrators. It underlines why Salesforce data backup is critical to prevent data loss, ensures compliance and enables fast recovery by providing a comprehensive, purpose-built

Salesforce backup solution that gives organizations the ability to recover from Salesforce data loss with speed and confidence.

MANAGEENGINE UNVEILS CLOUD-BASED REMOTE MONITORING AND MANAGEMENT SOLUTION FOR ENDPOINTS

ManageEngine, the enterprise

IT management division of Zoho Corporation, has announced the launch of Endpoint Central MSP Cloud, which brings the advantages of the cloud's scalability, flexibility, and efficiency to the remote monitoring and management (RMM) of endpoints for managed service providers (MSPs). The launch also completes the first stage of the company's vision for a unified platform for MSPs.

MSPs need a holistic solution for remotely monitoring and managing clients' desktops, servers, laptops and mobile devices from a central location. However, on-premises solutions come with scalability constraints and increased



upfront expenses, hampering business growth. Shifting to a cloud solution offers MSPs the flexibility to scale up their resources as needed, ensuring IT costs align with their actual needs.

"This cloud release enables service providers to focus on addressing their clients' IT challenges and growing their businesses without the worry of operational complexities," said Mathivanan Venkatachalam, vice president of ManageEngine. "Endpoint Central MSP Cloud delivers RMM capabilities for endpoints, enabling MSPs to automate everyday management and security tasks and allowing them to be available to help clients with their real-time requirements," he added.

VECTRA AI ADDS ADVANCED HYBRID ATTACK DETECTION, INVESTIGATION AND RESPONSE CAPABILITIES FOR AWS

Vectra Al, Inc., the leader in hybrid attack detection, investigation and response, has announced advancements to the Vectra Al Platform with the introduction of enhanced Cloud Detection and Response (CDR) for AWS environments. Armed with Vectra Al's patented Attack Signal Intelligence, Vectra CDR for AWS empowers security operations center (SOC) teams with realtime, integrated attack signal for hybrid attacks spanning network, cloud and identity domains.

As enterprises continue to move applications, workloads, and data into cloud environments, hybrid attack detection, investigation and response has become increasingly siloed and complex. According to Vectra AI's 2023 State of Threat Detection report, 90% of SOC analysts express a lack of confidence in their ability to keep pace with the increasing volume and variety of threats — 71% expressing concerns that their organizations have already been the target of a compromise that they are yet unaware of. Additionally, 75% of SOC analysts say they don't have the visibility they need to adequately defend their organizations.

What's more, the growth in hybrid deployments has added significant challenges for enterprise SOC teams. While attacker goals remain the same, attacks in the cloud manifest differently from those in traditional data center environments. Threats in the cloud focus primarily on credentials, leverage shallow kill chains and move faster compared to those observed onpremises. The same dynamic nature



of the cloud enables faster innovation; however, attackers also leverage this advantage to infiltrate and compromise environments in similarly innovative ways. These fundamental differences in how attacks manifest mean defenders need to think like hybrid attackers to effectively defend the growing hybrid attack surfaces they are called on to protect.

TRELLIX REPORT HIGHLIGHTS NEW PROGRAMMING LANGUAGES IN MALWARE DEVELOPMENT

Trellix, the cybersecurity company

delivering the future of extended detection and response (XDR), has released The CyberThreat Report: November 2023 from its Advanced Research Center. Trellix observed indicators of collaboration between ransomware groups and nation-statebacked advanced persistent threat (APT) actors, adoption and usage of lesserknown programming languages for malware, and cybercriminals developing Generative AI (GenAI) tools.

"As technology advances, so does cybercrime — and understanding the changing landscape is vital for CISOs and SecOps teams to stay ahead of threats," said John Fokker, Head of Threat Intelligence, Trellix Advanced Research Center. "Cybercriminals are becoming increasingly more agile, organized, and politically aligned. It is imperative defenders refer to threat intelligence to strengthen their security posture with limited resources."

The cybersecurity landscape experiences upheaval regularly as geopolitical and economic developments create an increasingly complicated and uncertain world. New cyber actors emerge daily while new vulnerabilities, exploits, and tactics are constantly discovered. The comprehensive analysis provided by



the Trellix Advanced Research Center serves as a vital resource for today's CISOs to understand and mitigate evolving cybersecurity risks in an interconnected world.

MORE THAN 120,000 UAE SCHOOL STUDENTS PARTAKE IN CYBERSECURITY AWARENESS PROGRAM TO MARK CYBER DEFENSE DAY

The UAE Cyber Security Council,

in collaboration with Core42 and KPMG, has announced the launch of Cyber Defense Day – an innovative educational initiative designed to equip young people with cybersecurity preparedness.

The virtual gamified event will be held on November 16, with the collaboration of strategic partners the Education and Human Resources Council, Ministry of Education, Emirates Schools Establishment, Department of Education and Knowledge, Sharjah Private Education Authority, and the participation of Dubai private schools. It will bring together over 120,000 grade 5-8 students, as they attempt to establish a nationwide campaign through a custom-designed 'Minecraft Education' game, which



will teach them to safeguard against cyber-attacks. The initiative has already secured the participation of over 520 school champions (teachers) who will collaborate on coordinating within each school. Dr. Mohamad Al Kuwaiti, Head of the UAE Cyber Security Council, said:

"Empowering students against the risks and dangers of cyber-attacks is a vital step to ensure the safety of our citizens. We are delighted to have schools across the UAE join us in this crucial initiative to build cyber resilience at the grassroots level."

He emphasized the initiative's commitment to addressing emerging cybersecurity threats, including advanced malware attacks using artificial intelligence. Dr. Mohammed also expressed his enthusiasm that

the initiative aligns with the UAE's 50 initiatives, promoting a safer digital future and culture.

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.





20 Ah

HIKVISIONMENA

4G

in HIKVISION-MENA



HIKVISION



Scan to Learn More

KYNDRYL UNVEILS BANKING & FINANCIAL INDUSTRY SERVICES FOR GOOGLE CLOUD CUSTOMERS

yndryl, the world's largest technology infrastructure services provider, has announced the availability of new services for financial services organizations seeking to use Google Cloud to safely store and protect their confidential and sensitive data. Kyndryl's new services are designed to enable a unified, scalable and security-rich data platform to

support customers' regulatory and

compliance activities and requirements. Kyndryl developed the new services on Google Cloud's reference architecture for financial services, with a focus on automation, security, and making compliance easier for customers. Customers can utilize Google Cloud's security solutions, such as Confidential Computing to encrypt their confidential data p, and Google Cloud Security Command Center to identify vulnerabilities and detect threats.

Kyndryl's financial services implementation for Google Cloud is tailored to meet the unique requirements and compliance standards of the financial industry. The new services feature many capabilities and differentiators essential to helping banks and financial institutions digitally modernize, including Kyndryl Consult architects and engineers; Kyndryl's experienced developer and delivery teams; Kyndryl Cloud Native Managed Services; and Kyndryl compliance and security expertise.

With its modular, industry experiencebased approach designed for cloud security and privacy, Kyndryl is partnering with Google Cloud to meet the needs of financial services



customers via an industry cloud approach that overcomes the inadequate and limited capabilities of generic services.

"We have developed innovative services with advanced security capabilities to help financial services organizations plan and implement their data and application environment in Google Cloud," said Meenagi Venkat, Vice President, Kyndryl Consult, Cloud. "Kyndryl's 30+ years of experience with designing, building and managing mission-critical IT infrastructures provides customers the assurances they need to ensure they run and transact their businesses in the cloud with confidence and security."

"Services partners like Kyndryl provide the ongoing expertise and resources that many enterprises need for large-scale digital transformation projects," said Benjie Harrison, Director of Global Alliances, Google Cloud. "Kyndryl will now provide financial services companies with new solutions that apply Google Cloud's trusted infrastructure and security tools to help customers achieve their business transformation goals."

To enable a rapid and smooth transition to Google Cloud for financial services customers, Kyndryl has focused on key enablers, such as an industry-specific design that accelerates onboarding. The services enable customers to adopt modern operations practices such as Infrastructure as code (IaC) and can be adapted to specific customer requirements and local regulatory requirements and helps customers confidently and securely build and solve business challenges.

Kyndryl also applied its deep industry expertise and cloud native capabilities to create dynamic financial services based on an operating model that continuously governs and optimizes performance, aligns cloud pricing and spend with business outcomes, and provides composable cloud services that facilitate faster solutioning and time to revenue.



Bedata 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

SECURIT IN THE IN THE DIGITAL AGE

SECURITY ADVISOR MIDDLE EAST TAKES A NEXT-GENERATION APPROACH TO CYBERSECURITY AND ANALYSES THE VARIOUS THREATS, TRENDS AND DEFENCE MECHANISMS AT PLAY.

0 1101010 001

010100

0101

0000111100010 01



n the digital age, where the pulse of society beats in binary code, the symbiotic relationship between Artificial Intelligence (AI) and cybersecurity is more pivotal than ever. As we witness unprecedented technological advancements, the stakes of protecting our digital infrastructure against malicious actors have reached new heights. Al emerges as both a formidable ally and a potential double-edged sword in the realm of cybersecurity.

On the positive front, Al brings a transformative paradigm shift to cybersecurity, enhancing our ability to detect and respond to threats with unprecedented speed and precision. Machine learning algorithms analyse vast datasets, identifying patterns and anomalies that human analysts might overlook. This proactive approach allows for the swift identification of potential vulnerabilities, enabling preemptive actions to fortify digital defenses. Aldriven threat intelligence also empowers organisations to stay ahead of the curve, adapting to evolving cyber threats in real-time.

However, the power of Al in the hands of malevolent actors poses an equal, if not greater, risk. Al is now being exploited by hackers to create more sophisticated and elusive attacks. The dark side of AI has ushered in a new era of cyber threats, challenging traditional defense mechanisms and raising the stakes for organisations and individuals alike.

One of the primary ways hackers leverage AI is through the creation of malicious algorithms that can adapt and evolve in response to changing security measures. Machine learning algorithms enable malware to learn from its environment, making it increasingly adept at avoiding detection by traditional antivirus software. This adaptive capability allows cybercriminals to deploy polymorphic malware that shape-shifts, making it a moving target for cybersecurity defenses.

Automated phishing campaigns have also become more convincing with the assistance of AI. Hackers employ natural language processing algorithms to craft phishing emails that mimic human communication styles, making them more difficult for recipients to discern from legitimate messages. AI-driven social engineering attacks capitalise on the analysis of vast datasets to tailor manipulative tactics, preying on human vulnerabilities and increasing the success rate of these deceptive endeavors.

Deepfakes, another ominous manifestation of AI in the hands of hackers, enable the creation of hyper-





realistic forged content, such as videos and audio recordings. This technology can be exploited to impersonate individuals, including high-profile figures, for malicious purposes, sowing discord or spreading misinformation on an unprecedented scale.

The acceleration of Al-driven cyber threats necessitates a proactive and adaptive cybersecurity approach. Defenders must harness the same technology to develop advanced threat detection systems capable of outsmarting



these malicious algorithms. As the battle between cybersecurity professionals and hackers unfolds in the digital realm, the responsible and ethical use of AI becomes imperative to ensure that the very technology designed to protect us does not inadvertently become a weapon in the wrong hands.

Navigating this delicate balance requires a multi-faceted approach. Policymakers must foster international collaboration to establish ethical frameworks governing the use of AI IN THE EVOLVING LANDSCAPE OF CYBERSECURITY, THE FUSION OF HUMAN INTELLIGENCE WITH → AI CAPABILITIES IS NOT JUST AN OPTION BUT A NECESSITY. in cybersecurity. The development of standardized protocols and regulations can ensure that AI technologies serve the collective interest while mitigating potential risks. Simultaneously, investment in AI education and training programs is paramount to cultivating a workforce equipped to harness the full potential of these technologies responsibly.

In the evolving landscape of cybersecurity, the fusion of human intelligence with AI capabilities is not just an option but a necessity. As we stand at the crossroads of innovation and security, a harmonious integration of AI into our defense strategies is the key to safeguarding the digital realm for generations to come.

Let's now explore the gamechanging benefits of AI in the realm of cybersecurity, shedding light on how these intelligent systems are reshaping the future of digital defence.

1. Swift Detection and Response

Al's ability to analyse massive datasets at lightning speed has revolutionised threat detection and response. Machine learning algorithms can identify patterns, anomalies, and potential vulnerabilities with a level of efficiency that surpasses traditional methods. The result? Cyber threats are identified and neutralised in real-time, preventing potential breaches before they can wreak havoc.

2. Proactive Threat Intelligence

Imagine having a crystal ball that predicts cyber threats before they materialise. Aldriven threat intelligence does just that. By continuously analysing global data trends and emerging threat landscapes, Al equips cybersecurity professionals with the foresight needed to anticipate and counteract evolving cyber threats,

AI'S ABILITY TO ANALYSE MASSIVE DATASETS AT LIGHTNING SPEED HAS REVOLUTIONISED THREAT DETECTION AND RESPONSE.

A HARMONIOUS INTEGRATION OF AI INTO OUR DEFENSE STRATEGIES IS THE KEY TO > SAFEGUARDING THE DIGITAL REALM

staying one step ahead of the adversary.

3. Automated Defense Mechanisms

Al doesn't just identify threats; it actively fortifies digital defenses. Automated response mechanisms powered by Al can neutralise threats autonomously, reducing the burden on human analysts and allowing for faster and more accurate countermeasures. This integration of human-machine



16 NOVEMBER 2023





ONE OF THE → PRIMARY WAYS HACKERS LEVERAGE AI IS THROUGH THE CREATION OF MALICIOUS ALGORITHMS.

collaboration ensures a dynamic defense strategy that adapts to the ever-changing cybersecurity landscape.

4. Enhanced Data Security and Privacy

Al algorithms excel at identifying sensitive data and safeguarding it from unauthorised access. From predictive analysis to anomaly detection, Al technologies contribute to the creation of robust data protection frameworks, ensuring that personal and organisational information remains confidential and secure.

5. Redefining Cybersecurity Workforce Dynamics

With AI handling routine tasks and augmenting human capabilities, cybersecurity professionals can focus on high-level strategic thinking and decision-making. This shift in workforce dynamics enhances overall efficiency, empowering experts to address complex challenges and devise innovative solutions.

As we navigate the intricate web of digital threats, AI emerges as the linchpin in fortifying our defenses. This cover story delves into the transformative impact of AI on cybersecurity, unraveling the tapestry of benefits that this groundbreaking technology brings to the forefront of the ongoing battle for a secure digital future.

A NEW APPROACH TO SECURITY – SHIFTING ZERO TRUST TO IMPROVE EMPLOYEE WELLBEING

SPENCER PITTS, EMEA CHIEF DIGITAL WORKSPACE TECHNOLOGIST, VMWARE

s people are now working more and more distributed and or in a hybrid workplace, new and existing threats, such as social engineering phishing attacks and ransomware, continue to develop and target people working this way. To protect themselves, organisations must remain vigilant and maintain a healthy security posture of course, but has there been an unintended impact on businesses and their people? Have security practices moved on over the last few years to enable greater worker freedom or have they reverted to a 'lock down everything' approach of old but under a new name... 'Zero Trust'?

Businesses have needed to question the most established security practices to maintain flexibility, especially now in the norm of hybrid. A 'Zero Trust security' methodology has emerged as the desired approach to protecting the businesses and the way they operate today. At the core of the Zero Trust principle from a user access perspective is that they, and their devices, are treated as hostile at first until verification and authentication, proves otherwise (and continuously) – thereby establishing trust. This is also known as 'never trust always verify' or the 'least privilege' concept. In theory then we can apply this in a way that means we can cater for people accessing information and applications regardless of location, in or outside the office. The question though is, are we doing it right?

In reality, what tends to happen is the model is implemented in a way that organisations often impose the same rigid rules on all employees but maybe this time round they filter to 'outside the of the office' –



whether they're regularly accessing sensitive corporate data or not. Many don't take individual job functions into account when mapping the risk and, therefore, it doesn't trust anyone. This can be productivity limiting for those performing considerably "safer or less risky" roles. For instance, does it make sense in holding the person delivering your parcels to the exact same corporate security standards as an office-based VP of a business, especially if that process for access is time consuming?

Zero Trust done badly can mean putting security above all other aspects of the business, including individual job functions and the organisation's overall need to focus on user experience, agility and innovation.

On a much more day-to-day level, the more draconian organisations are with their implementation of Zero Trust, the more backlash they may face from employees. Understandably, if an employee's job functions are being disrupted by tight security controls, they're going to find ways around it – which can create a whole host of new security issues.

Organisations should look to adopt a bespoke or tailored approach to Zero Trust, leverage Zero Trust principles but combine this with risk profiling, treating users and devices with the scrutiny reflective of their job function plus the data they need to access. It's a 'persona-driven' approach which places the individual – rather than just the organisation – at the heart of the process, to provide a more flexible experience, without compromising security.

There are several key elements to consider with this approach. The first step is understanding the job function and then the associated risk in relation to the apps and data the required to be



accessed as part of that persons working day. These risks might be location, the data sensitivity, the device being used etc. The Zero Trust model has five main pillars of risk context and context is important here.

The other important part of the Zero Trust thinking is the concept I mentioned earlier, which is always verify. This part done badly can have a massive impact on the experience received. Imagine going to a restaurant for a meal, you've booked under your name and get asked for I.D at the front desk when you arrive. That sounds reasonable of course, now imagine that every five minutes the waiting staff ask you again to show your I.D. I'm thinking that eating experience might live long in the memory and not for the right reasons.

So, would we want the same then for our employees simply trying to do their jobs but constantly asked for authentication? There must be a balance, an appropriate level applied based on risk and importantly if that

risk changes. Up until recently how you collect information, the timeliness of and then apply context in terms of risk has been difficult. Technology has advanced here and the rise of Machine Learning in this area means we can make decisions on risk more quickly and this will help make the 'always verify' part of Zero Trust succeed. Back to our restaurant example, we can think of this as the staff only ask someone to show ID again if they notice they look completely different to the people who came in. In other words, look for changes, things out of place, we are verifying but in a way that does not impact the end person.

Finally, as an extension of Tailored Trust, businesses' approach to security training should reflect their overall security posture. Just as with any other form of training, security training ideally should be personalised to a specific job function or level. I wouldn't be surprised if employees switch off after hours of security training that isn't relevant to them, which creates further problems for IT teams down the line. At Rentokil Initial, the company splits its workforce into different personas based on their existing knowledge of cyber security, helping to identify which workers need which type of training. 1

A 'ZERO TRUST SECURITY' METHODOLOGY HAS EMERGED AS THE DESIRED APPROACH TO PROTECTING THE BUSINESSES AND THE WAY THEY OPERATE TODAY.

ACRONIS HELPS MANAGED SERVICE PROVIDERS GROW BY INTRODUCING MSP ACADEMY



cronis, a global leader in cyber protection, has announced the launch of MSP Academy, an educational initiative aimed to provide managed service providers (MSPs) with business and technological knowledge, skills, and tools necessary to excel and grow. The MSP Academy launch represents a significant expansion of Acronis' educational offerings, delivering on the commitment of Acronis to support the development of the global MSP market.

Acronis has offered extensive technology and business training on Acronis products for service providers for over ten years through Acronis Academy. Acronis partners that went through training and certification through the Academy in 2022 saw a 60% increase in revenue from Acronis product sales and a reduction in support incidents by 40%. In response to partner requests to expand the training portfolio beyond product training, Acronis delivered MSP Academy.

MSP Academy is a learning platform created to address key challenges MSPs face. It covers various topics, from starting an MSP, running a successful MSP business, marketing an MSP business, and optimising the

efficiency and productivity of MSP technicians.

"MSP Academy offers a customised education experience, allowing learners to explore specific topics or follow a structured learning path," said Jon McCarrick, Director of Evangelism at Acronis. "The rapidly evolving technology and business landscape

ACRONIS MSP ACADEMY IS A COMPREHENSIVE TRAINING PROGRAM DESIGNED FOR MANAGED SERVICE PROVIDERS, COVERING BUSINESS OPERATIONS, TECHNOLOGY, SALES, AND MARKETING.



Acronis MSP Academy

requires ongoing learning, and MSP Academy is designed to support the growing needs of MSPs."

MSP Academy's curriculum is crafted to offer training covering all aspects of managing an MSP business. With content structured to cater to the fastpaced changes of technology, bitesized modules ranging from three to seven minutes are available to deliver impactful insights. Participants can take an exam to receive a Credly badge to share with peers and customers, showing their qualifications and commitment to continuous learning by earning a degree from the MSP Academy.

Upcoming initiatives from Acronis

include delivering hybrid boot camps in collaboration with cloud distributors, providing an immersive learning experience to keep learners at the forefront of industry advancements, and launching new online, hybrid, and offline multilingual training options, ensuring that MSPs across the world can benefit from the program.

AFRICAN-EASTERN PARTNERS WITH SECUREWORKS FOR CUTTING-EDGE SOC SERVICES

ANITA JOSEPH CAUGHT UP WITH **SANTOSH JOHN THOMAS**, CIO AT AFRICAN-EASTERN, TO DISCUSS THE COMPANY'S CYBERSECURITY JOURNEY AND ITS PARTNERSHIP WITH SECUREWORKS FOR CUTTING-EDGE SOC SERVICES.

an you provide an overview of your organisation's cybersecurity journey up to this point? What were some of the key milestones and challenges you encountered along the way?

African + Eastern, a name synonymous with excellence, boasts a remarkable history spanning more than three centuries, first as a general trading company originating in Africa and more recently in the Middle Eastwith in excess of 50 years expertise exclusively in the distribution of alcoholic beverages in the Arabian Gulf. We proudly hold the distinction of being the leading distributor in our region across the key categories in which we operate.

Our cybersecurity journey began approximately 25 years ago when our organisation was relatively modest, comprising around 25 to 30 employees. At the time, our IT infrastructure was basic, featuring the PIX firewall, which was considered state-of-theart back then. However, our quest for cybersecurity excellence led us to progressively enhance our defences. We ventured into developing our inhouse firewall solutions and gradually integrated more robust security measures, such as perimeter firewalls, vulnerability assessments, intrusion prevention systems, and next-generation firewalls, among others. Over time, we diligently implemented these crucial components.

Yet, there came a point when we realised that the path we were on might not be the right one. Despite our extensive security infrastructure, we needed to shift our perspective. It was a turning point when we recognised the need for a comprehensive cybersecurity portfolio, viewed from a different angle. This realisation prompted us to embark on a new direction: establishing our very own Security Operations Centre (SOC). We initiated a thorough evaluation of various options, embarking on a journey to explore the realm of SOCs. This is how we reached where we are today, with a heightened focus on cybersecurity analysis and our ongoing journey in the world of SOCs.

Why did you decide to invest in a Security Operations Center (SOC) service for your organisation's cybersecurity needs? What were the driving factors behind this decision?

At African + Eastern, our IT department are structured into four key pillars. The first pillar is dedicated to IT operations and IT security, serving as the foundation of our technological framework. Our second pillar, the Enterprise team, focuses on managing ERP systems. The third pillar, the Digital Transformation team, is at the forefront of our technological evolution. Lastly, the newest addition to our portfolio is the Data Analytics team, which contributes to our data-driven decision-making.

Security is an exceptionally serious matter at African + Eastern, and it's a core aspect of our IT operations. As we assessed our security parameters, we came to realise that the various components we had in place, including

SECURITY IS AN EXCEPTIONALLY SERIOUS MATTER AT AFRICAN + EASTERN, AND IT'S A CORE ASPECT OF OUR IT OPERATIONS.

the CO firewall, perimeter firewall, vulnerability assessments, and nextgeneration EDR solutions, presented a significant challenge for our organisation. Despite our commitment to security, the complexity of our security infrastructure was a challenge we needed to address. Recognising this, we made the strategic decision to establish a dedicated Security Operations Centre (SOC). The SOC's primary role is to provide continuous, round-the-clock monitoring of our IT applications and endpoints throughout African + Eastern.

In our quest for the right SOC partner, we discovered Secureworks, a recognised leader in the field of security operations centres in our region. Our discussions with them culminated in a collaborative partnership. Today, we can confidently state that we've entrusted our security operations to Secureworks, effectively transferring and mitigating our security risks.

What specific security goals or objectives were you looking to achieve by implementing a SOC service? Are there any particular threats or risks that prompted this move?

Initially, there was a noticeable absence of dedicated personnel overseeing security matters in our organisation. While we had various security tools in place, the critical element of vigilant monitoring was lacking. Given the expansive nature of African + Eastern's IT landscape and our substantial size, we faced the challenge of not having a dedicated resource to comprehensively analyse the vast array of logs generated. This realisation prompted us to take action, recognising the pressing need for rigorous monitoring of our secure development practices. Thankfully, we've experienced a relatively secure environment thus far, thanks in part to regular security audits. However, these audits also underscored that while we were secure, we had not reached the level of security we aspired to attain. Consequently, we arrived at the decision that establishing a Security Operations

IN OUR QUEST FOR THE RIGHT SOC PARTNER, WE DISCOVERED SECUREWORKS, A RECOGNISED LEADER IN THE FIELD OF SECURITY OPERATIONS CENTRES IN OUR REGION.

Centre (SOC) was imperative to provide continuous, 24/7 monitoring of African + Eastern's entire IT landscape.

Can you explain the timing behind the decision to implement a SOC service? What factors influenced the decision to do it now?

The need for a Security Operations Centre (SOC) became evident as the world and African + Eastern grappled with the challenges posed by the pandemic. Internally, numerous debates took place, leading to a year-long deliberation on the best course of action. The central question revolved around whether to invest in establishing an in-house SOC or continue to acquire and manage the various security components independently. During this period, we continued our investments in other security areas, attempting to find the right balance.

However, a pivotal moment occurred when it became clear that our current approach was inadequate. We realised that the threat landscape was continually evolving, and merely investing in isolated security solutions was not a sustainable strategy. This realisation led to the unanimous decision that a dedicated SOC was imperative. After over a year of careful consideration and evaluation of numerous potential partners, we ultimately chose to collaborate with Secureworks. Their global expertise and comprehensive SOC services aligned perfectly with our security requirements and vision for the future.

What were the key considerations that led you to choose Secureworks as your SOC service provider? Were there any unique features or capabilities that stood out to you?

Our decision to partner with Secureworks

was shaped by several critical considerations. Firstly, the reliability of their XDR (Extended Detection and Response) platform, known as "Taegis™," stood out. This flagship platform proved to be exceptionally effective during our rigorous evaluation process. It offered comprehensive threat detection and correlation rules, which impressed us greatly. This level of effectiveness left no room for doubt in our discussions, making it abundantly clear that Secureworks could meet our security requirements.

Secondly, our interactions with the local team at Secureworks, led by Gopan Sivasankaran, underscored their distinct advantage. Gopan's local presence set them apart, unlike many other SOC service providers in the region who lacked a senior resource on-site. This local presence was particularly valuable in cases requiring swift escalation, such as responding to security incidents or potential breaches. We found this aspect to be a crucial parameter when assessing the suitability of a partner.

The third vital factor that weighed in favour of Secureworks was the depth of expertise they brought to our region. Our interactions with their local technical team left us thoroughly impressed. Their knowledge and support, especially during a proof of concept, exceeded our expectations. At no point during this process did we doubt our decision

A SOC IS NOT MERELY THE ENDGAME IN THE EVER-EVOLVING → LANDSCAPE OF CYBERSECURITY. to partner with Secureworks. Their combination of expertise, resources, leadership, and a robust platform made them the clear choice as the right partner for African + Eastern in the realm of SOC services. Hence, we confidently selected Secureworks for our SOC journey.

How does the Secureworks SOC service align with your organisation's broader cybersecurity strategy and objectives?

At African + Eastern, we hold security in the highest regard, recognising its paramount importance. This perspective is mirrored by Secureworks, making our conversations about our security objectives seamlessly aligned. We embarked on discussions at a broad level, delving into our security priorities, and found a remarkable resonance with the approach taken by Secureworks. This synergy enabled us to chart out our objectives and correlate them with the metrics and strategies they had to offer.

Secureworks, with its wealth of expertise, introduced valuable insights into our discussions. We found ourselves in strong agreement on critical aspects such as incident response, threat hunting, and the validity of security measures. The cohesion between their proposals and our organisational objectives was evident. Following these discussions, we swiftly solidified our partnership with Secureworks, marking the beginning of a mutually beneficial journey. Their commitment to security aligns perfectly with our vision, making them an ideal collaborator in our pursuit of safeguarding our organisation.

In what ways do you envision the SOC service evolving to meet the changing threat landscape and your organisation's evolving security needs?

Every organisation, regardless of its size, whether small, medium, or largescale, requires a dedicated Security Operations Centre (SOC). The choice between establishing an in-house SOC or opting for a global partner depends on the organisation's specific needs and preferences. However, it's essential to recognise that a SOC is not merely the endgame in the ever-evolving landscape of cybersecurity.

Hackers continually devise sophisticated strategies to breach an organisation's defences. To effectively combat these evolving threats, a SOC must be dynamic and mature, capable of adapting to the changing threat landscape. In my perspective, the evolution of SOCs is an ongoing journey. We should encourage the development of multiple SOC players across the world, fostering the creation of comprehensive threat databases and threat vectors. It's a path that needs to be nurtured and refined over time to keep pace with the evolving threat landscape and safeguard organisations effectively.

What advice would you offer to other CIOs or organisations considering a similar path towards enhancing their cybersecurity through SOC services and providers like Secureworks?

African + Eastern has always recognised the importance of security. Yet, due to various challenges, including resource constraints, user-friendliness concerns, and budget limitations, the journey towards bolstering our security measures was complicated. It's a challenge shared by many organisations in this region, where security is often viewed as an expensive necessity, rather than a readily embraced priority. Some might question the substantial investments in security, asking why such extensive measures are essential.

In response, I'd pose a simple question: Why do we take out insurance for our

A VITAL FACTOR THAT WEIGHED IN FAVOUR OF SECUREWORKS → WAS THE DEPTH OF EXPERTISE THEY BROUGHT TO OUR REGION. personal lives? The same principle applies to our organisations. In a rapidly evolving security landscape, where new threats and vulnerabilities emerge daily, investing in security is akin to securing insurance for our digital existence. It's an indispensable safeguard that shouldn't be overlooked. Cybersecurity is not a destination but an ongoing journey, one that necessitates continuous investments, the right expertise, alignment with business goals, and support from management to ensure that your organisation remains well-protected in the complex realm of application security.

Tell us about your partnership with Finesse

As we began our search for the ideal SOC partners, we swiftly recognised Secureworks as one of the foremost choices in this region. Their global and local presence made them a strong contender. However, we understood that this wasn't the entire solution; we required a local SOC partner to address our specific needs. This realisation prompted us to explore how we could further enhance our security infrastructure beyond Secureworks.

Enter Finesse—a significant addition to our cybersecurity equation. Engaging in discussions with Finesse, who acts as a direct partner of Secureworks, was a pivotal moment in our journey. Finesse boasts deep expertise in the platform provided by Secureworks, offering the local support we required. This collaboration provided us with a seamless and efficient avenue for bolstering our security.

Since African + Eastern doesn't maintain an in-house security team, we entrusted Finesse with the task of managing our security operations. Their proficiency of the Secureworks platform, combined with the local presence of Finesse in Dubai, has contributed immensely to keep us safe and secure. Should any security issue arise, we know exactly who to contact first and have a well-defined protocol for escalation. Finesse has proven to be the right partner in our ongoing cybersecurity journey. **1**



CYBERCRIMINALS DISABLED OR WIPED OUT LOGS IN 82% OF ATTACKS WITH MISSING TELEMETRY: SOPHOS

38% OF "FAST" RANSOMWARE ATTACKS IN REPORT OCCURRED WITHIN 5 DAYS OF INITIAL ACCESS ophos, a global leader in innovating and delivering cybersecurity as a service, has released its Active Adversary Report for Security Practitioners, which found that telemetry logs were missing in nearly 42% of the attack cases studied. In 82% of these cases, cybercriminals disabled or wiped out the telemetry to hide their tracks. The report covers Incident Response (IR) cases that Sophos analysed from January 2022 through the first half of 2023.

Gaps in telemetry decrease muchneeded visibility into organisations' networks and systems, especially since attacker dwell time (the time from initial access to detection) continues to decline, shortening the time defenders have to effectively respond to an incident.

"Time is critical when responding to an active threat; the time between spotting the initial access event and full threat mitigation should be as short as possible. The farther along in the attack chain an attacker makes it, the bigger the headache for responders. Missing telemetry only adds time to remediations that most organisations can't afford. This is why complete and accurate logging is essential, but we're seeing that, all too frequently, organizations don't have the data they need," said John Shier, field CTO, Sophos.

THE REPORT COVERS INCIDENT RESPONSE (IR) CASES THAT SOPHOS ANALYSED FROM JANUARY 2022 THROUGH THE FIRST HALF OF 2023.

In the report, Sophos classifies ransomware attacks with a dwell time of less than or equal to five days as "fast attacks," which accounted for 38% of the cases studied. "Slow" ransomware attacks are those with a dwell time greater than five days, which accounted for 62% of the cases.

When examining these "fast" and "slow" ransomware attacks at a granular level, there was not much variation in the tools, techniques, and livingoff-the-land binaries (LOLBins) that attackers deployed, suggesting defenders don't need to reinvent their defensive strategies as dwell time shrinks. However, defenders do need to be aware that fast attacks and the lack of telemetry can hinder fast response times, leading to more destruction.

"Cybercriminals only innovate when they must, and only to the extent that



it gets them to their target. Attackers aren't going to change what's working, even if they're moving faster from access to detection. This is good news for organizations because they don't have to radically change their defensive strategy as attackers speed up their timelines. The same defenses that detect fast attacks will apply to all attacks, regardless of speed. This includes complete telemetry, robust protections across everything, and ubiquitous monitoring," said Shier. "The key is increasing friction whenever possible—if you make the attackers' job harder, then you can add valuable time to respond. stretching out each stage of an attack.

"For example, in the case of a ransomware attack, if you have more friction, then you can delay the time until exfiltration; exfiltration often occurs just before detection and is often the costliest part of the attack. We saw this happen in two incidents of Cuba ransomware. One company (Company A) had continuous monitoring in place with MDR. so we were able to spot the malicious activity and halt the attack within hours to prevent any data from being stolen. Another company (Company B) didn't have this friction; they didn't spot the attack until a few weeks after initial access and after Cuba had already successfully exfiltrated 75 gigabytes of sensitive data. They then called in our IR team, and a month later, they were still trying to get back to business as usual."

The Sophos Active Adversary Report for Security Practitioners is based on 232 Sophos Incident response (IR) cases across 25 sectors from Jan. 1, 2022, to June 30, 2023. Targeted organisations were located in 34 different countries across six continents. Eightythree percent of cases came from organisations with fewer than 1,000 employees.

The Sophos Active Adversary Report for Security Practitioners provides actionable intelligence on how security practitioners should best shape their defensive strategy.

REDEFINING DATA MANAGEMENT

MICHAEL CHANG,

REGIONAL MANAGER AT SYNOLOGY INC, TELLS ANITA JOSEPH ALL ABOUT HOW THE COMPANY IS REDEFINING DATA STORAGE, ACCESS, PROTECTION AND MANAGEMENT WITH ITS CUTTING-EDGE PRODUCTS AND SOLUTIONS.

> hat was the theme of your participation at GITEX this year, and what were the key aspects you highlighted at the show?

This year at GITEX, we're showcasing our comprehensive IT solutions that span edge, core, and cloud environments. We have set up four dedicated zones to emphasise different aspects of our offerings.

Enterprise Storage and Data Management:

The demand for data storage and management in enterprises has significantly increased with the emergence of new technologies like generative artificial intelligence. Synology is well-prepared to address high-performance requirements, including virtualisation environments, big data analytics, and deep learning. We have expanded our portfolio to cater to enterprise scenarios, introducing the FS



Series all-flash storage solutions for latency-sensitive workloads, the SA6400 for future expansion, and the HD6500 designed for PB-level storage needs.

In addition to expanding storage capacity, Synology is continually enhancing data security measures. The incorporation of the latest 7.2 version of DiskStation Manager empowers businesses with advanced tools like full-volume encryption and Immutable Snapshots, leveraging write once read many (WORM) technology to safeguard data from malicious attacks, tampering, and accidental deletions by creating an unalterable copy of their data.

Data Protection and Disaster Recovery Solutions:

We offer license-free backup solutions that support data backup across different platforms, including physical servers, virtual machines, PCs, Google Workspace, and M365, all through a single portal. This ensures that critical business data is regularly backed up and can be quickly restored in case of data loss or system failure.

We're also excited to announce an innovative project focused on enhancing a streamlined data protection solutions for businesses. This project will be unveiled next year, so stay tuned!

End-to-End Smart Surveillance System:

Our end-to-end smart surveillance solution features from footage archiving, centralised video management system, to AI-powered cameras with high-quality, stable, 24/7 recording and built-in AI recognition enabling organisations to detect people, vehicles, and space intrusions. Additionally, the Deep Learning NVR Series enables businesses to perform advanced analytics including people & vehicle counting and facial recognition.

Cloud Solutions:

Synology's secure C2 cloud infrastructure, which offers password management, backup and recovery, secure file sharing, identity and access management, and scalable object storage with S3 compatibility. These solutions are deeply integrated with Synology's on-premises systems to create an efficient and reliable hybrid cloud infrastructure.

What are the challenges and opportunities in the 'AI Everything' landscape, and how do you aim to

support organisations in this journey?

The 'AI Everything' landscape presents several challenges and opportunities for organisations, particularly in terms of their IT infrastructure:

Challenges:

Big Data Volume: Al applications require vast amounts of data. Efficiently managing, storing, and processing this data is a significant challenge, especially as data generation rates increase rapidly.

Performance Requirements: Al

workloads demand high-speed data access and processing capabilities. Storage systems need to meet these performance demands without compromising latency.

Data Accessibility and Availability:

Ensuring data is readily accessible for training and inferencing processes is crucial. This requires robust storage solutions that provide high availability and fault tolerance.

Data Security and Compliance: As

AI applications often handle sensitive information, storage solutions must maintain robust security measures to protect data integrity and confidentiality.





As previously mentioned, Synology is well-prepared to address these challenges:

For Big Data Volume, our storage solutions, such as the SA6400 and HD6500, seamlessly scale as needed to meet the increasing demands of big data volume.

For Data Accessibility and Availability, Synology's integrated backup solutions provide a robust framework for ensuring data accessibility and availability. This enables organisations to implement effective backup and disaster recovery plans, guaranteeing uninterrupted access to data even in the face of a disaster.

For Data Security and Compliance, Synology NAS ensures data security and compliance with global regulations like GDPR. We also employ robust security measures including access control, encryption, Write Once Read Many (WORM) Technology and maintain a dedicated Security Incidence Response Team (SIRT) for user data safety.

With over two decades of leadership in NAS technology, what technologies and future products are you working toward in the next stage?

Synology is committed to addressing the top three challenges faced by businesses in the upcoming years: "Access," "Management" and "Protection."

Flexible Accessibility: The demand for storage continues to grow, driven by AI and other data-centric applications. Synology will help businesses scale up their storage capacity efficiently while also enabling them to scale out their storage by integrating multi-platform resources to accommodate the flexibility of growing data

Management Simplicity: As organisations grow, data is exchanged between various locations. Synology will integrate single pane-of-glass management into our ecosystem to help businesses achieve operational simplicity.

Data Protection: In an evolving threat landscape, data security is crucial.

SYNOLOGY IS WELL-PREPARED TO ADDRESS HIGH-PERFORMANCE REQUIREMENTS, INCLUDING VIRTUALISATION ENVIRONMENTS, BIG DATA ANALYTICS, AND DEEP LEARNING.

Synology offers comprehensive backup solutions to safeguard business data, and we're working on an exciting new project focused on streamlining data protection experiences for businesses.

Our solutions have already benefited over 50% of Fortune 500 businesses worldwide. Moving forward, we are eager to extend our support to more businesses in the Gulf region, helping them effectively manage and safeguard their data.

How important is an event like GITEX Global for your company – and how much value does it drive for your organisation?

Over the years, we see great potential in the MEA market. Our YoY growth have achieved over 30%, and we are expecting more growth this year. Participating in regional iconic tradeshow like GITEX offers opportunity for us to present our enterprise-ready products and solutions to a diverse and international audience. It also allows us to receive direct feedback from our users which helps in validating our offerings and gaining insights into potential areas for improvement.

It is a great platform for enhancing our brand's credibility and reinforces our position as an industry leader, and drive potential business opportunities.



Complexity Impacts Effective Security Eliminate Complexity through Convergence and Consolidation Enabled by the Fortinet Security Fabric

Cybersecurity, everywhere you need it





Copyright ©2023 Fortinet, Inc. All Rights Reserved.

POSITIVE TECHNOLOGIES: RANSOMWARE GANGS THREATEN TO PUBLISH VICTIMS' DATA

DOUBLE LISTING AND "LAWFUL EXTORTION": RANSOMWARE OPERATORS' NEW TACTICS

ositive Technologies experts have presented a study of the Q3 2023 cybersecurity threatscape. The share of malware attacks remained unchanged from Q2 at 45%. The advent of decryption tools reduced the effect of encryption malware, causing its share to shrink. Ransomware gangs now threaten to publish stolen information without encrypting the compromised systems or data. Experts are recording new methods employed by ransomware operators, including some unconventional social engineering techniques.

According to our analysis, Q3 2023 saw a slight decrease in the total number of cyberincidents from the previous quarter. With 37% of total incidents, exploitation of vulnerabilities remained a popular method for attacking organisations. Bad actors continued to take advantage of flaws in popular IT solutions, providing further evidence of the importance of regular updates and software security.

The share of malware attacks in Q3 2023 remained unchanged from the previous quarter at 45%. Throughout the quarter, cyberextortionists continued to demand ransoms for not disclosing information, while in several cases refraining from encrypting the data in the targeted systems.

"Encryption malware remains the most frequently used type of malware in attacks on organizations, but its share dropped by 6 percentage points from the previous quarter," says Alexey Novikov, head of the Positive Technologies Expert Security Center. "We believe that this drop can be attributed to the wider access to decryption tools and the fact that extortion gangs gradually forgo system and data encryption in favor of threatening to publish victims' data. In some cases, if the organization refuses to pay the ransom, the hackers reach out to its affected customers directly, trying to coerce them into paying for their data to be deleted. Double posting is another notable trend, where two ransomware gangs announce that they have successfully breached the same organisation, and each demands a ransom."

Novikov also noted a unique tactic used by the ransomware group Ransomed.vc. The group, which presents its malicious activities as a pentesting service, is abusing the European Union's General Data Protection Regulation (GDPR): should the victim refuse to pay up, the hackers publish the data they stole from the organisation, which results in it being fined for failure to protect the data. The expert named this tactic "lawful extortion".

According to Positive Technologies, the share of spyware attacks on individuals in Q3 increased to 65%. Spyware infections were detected in 20% of successful attacks on organisations, a figure that remains unchanged since Q2. More than half (57%) of all corporate infections with various types of malware occurred through email. Websites remained the main source of malware used to attack individuals at 49%, up 9 percentage points from Q2.

To protect devices against malware infection, experts recommend using sandboxes that allow analysis of file behavior in a virtualised environment, thereby detecting any malicious activity, and acting in time to prevent damage to the company. To protect against encryption attacks, regular backups are a must.

Social engineering remained the

THE SHARE OF MALWARE ATTACKS IN Q3 2023 REMAINED UNCHANGED FROM THE PREVIOUS QUARTER AT 45%.

biggest (92%) threat to private individuals and a major (37%) threat to organisations. Phishing scams continued to exploit the themes of employment, political turmoil, and making a quick buck (for example, by investing in cryptocurrencies), and also masqueraded as delivery services.

Positive Technologies experts highlight the fact that social engineering techniques never stop evolving. Bad actors used highly elaborate tactics to give their victims a false sense of security. Scammers used modular tools to craft convincing phishing sites and email reply chains; they also launched multistage attacks combining different cyberfraud techniques. Several attacks relied on compromised corporate IT systems to attack customers and business partners, as in the case of an attack on hotels listed on Booking.com. Positive Technologies predicts that AI-powered attacks will grow in number as more cybercriminals add the tool to their arsenals.

The experts recommend remaining vigilant online and refraining from opening suspicious links or downloading attachments from unverified sources. Users must treat with suspicion any urgent requests and offers that are too good to be true.

As in Q2, a data breach was the most common consequence of successful attacks on organizations (56%) and individuals (61%). Direct financial losses led as the second most common consequence (35%) for attacks on individuals. For organizations, disruption to core business functions was the second most frequent (36%) consequence of an attack, although its share decreased by 8 percentage points from Q2 as the use of data encryption by ransomware gangs declined. **1** INTERVIEW / ACRONIS

<complex-block>

AI-DRIVEN CYBER RESILIENCE

ANITA JOSEPH CAUGHT UP WITH **ALONA GECKLER,** SVP OF BUSINESS OPERATIONS & CHIEF OF STAFF AT ACRONIS TO FIND OUT HOW THE COMPANY INCORPORATES AI INTO ITS CYBER PROTECTION OFFERINGS.

an you tell us what you showcased at Gitex this vear? This year, we dedicated ourselves to the theme of "Empowering Cyber Resilience with AI." Our latest innovations have revolved around elevating cybersecurity and data protection, unveiling the most recent iteration of the Acronis Cyber Protect suite, designed to counter Al-powered threats proficiently. Alongside this, we introduced our next-generation cloud-based solutions and announced substantial partnerships aimed at bolstering their offerings. Our principal emphasis was on presenting the seamless incorporation of AI into our products, enabling proactive threat detection, and offering all-encompassing data protection solutions.

Additionally, we are proud to be the go-to solution for over 20,000 service providers globally. In our specific region, we work closely with over 300 service providers. GiTex serves as a vital gateway to the broader regional market.

What are your company's global plans for the future, particularly in the region?

Our global plans remain steadfast. We are committed to enhancing our product to make it a complete, all-inone solution. We've observed a growing demand in the market for a unified solution that service providers can integrate and offer to their customers, eliminating the need for separate backup, automation, and disaster recovery solutions. This is precisely what Acronis is dedicated to delivering. As an example, we recently introduced a new feature called EDR, which stands for Endpoint Detection and Response. In just one month, we successfully thwarted around 200,000 attacks with this feature. This showcases our constant drive for innovation. Furthermore, we heavily leverage AI in our products because cybercriminals are increasingly using AI. Only through AI-backed solutions



can we effectively combat these threats, as manual intervention becomes both expensive and complex. Our goal is to offer our service providers, who are often smaller companies with 10 to 20 employees, a ready-made solution that evolves and adapts to meet their needs. This enables them to offer comprehensive services to their customers.

Can you share more about the mentorship programs you've initiated, and how they've benefited women?

In industries traditionally dominated by men, like technology and cybersecurity, it's evident that the majority of participants are male. However, there's a growing trend to attract and retain more women in the industry. One of the key elements of our commitment to promoting diversity in the cyber field is the Acronis mentorship program, which we call #CyberDiversity. Each year, we identify approximately 50 highpotential women and pair them with our board directors, CEO, and other top-level executives. These women have the privilege of engaging in in-person mentorship sessions with these highprofile individuals, gaining valuable guidance and support. The mentorship program not only kick-starts their

professional development but also provides them with ongoing daily support. We've been running this program for two years now, and we've already seen remarkable examples of participants who have taken significant steps forward in their careers since joining the #CyberDiversity program.

What trends are you anticipating in 2024, especially in the realm of AI?

In 2024, we expect the trend of Al integration to persist and deepen. To that end, our engineers and product development are heavily focused on enhancing AI integration within our cyber protection solutions. We believe that AI will continue to play a crucial role in safeguarding organisations against cyber threats. Additionally, sustainability efforts, like environmentally friendly products, eco-conscious supply chains, and the embrace of renewable energy, will be vital for survival in the coming years. Furthermore, blockchain technology will also play an important role in Cybersecurity in the coming years. It has the power to transform various industries by boosting trust and efficiency through greater transparency and more robust security measures. It's an exciting frontier with enormous potential for positive change. ╏



A10 NETWORKS DETAILS SECURITY STRATEGY TO ADDRESS GROWING CYBER THREAT LANDSCAPE

istributed denial of service (DDoS) attacks continue to rise in frequency and sophistication. DDoSfor-hire, hacktivism and geopolitical forces all play a role in the growing cyber threat landscape. In fact, according to Gartner, DDoS attacks will be used as the most common cyberattack type in the coming years. And increasingly, threat actors are leveraging artificial intelligence (AI) to enhance the efficacy of DDoS attacks. This cyber threat landscape requires new and innovative approaches to DDoS defenses, those that leverage AI to help anticipate multi-vector attacks.

To help customers protect their networks and applications, meet uptime demands, deliver on customer expectations, and optimise secure experiences, A10 Networks (NYSE: ATEN) is establishing its A10 Defend security portfolio. This portfolio suite of products creates a holistic foundation for growth including new and advanced DDoS protection with AI-enhanced zero-day detection capabilities, analytics and proactive DDoS threat intelligence to protect against new and previously unknown attacks.

A10 Defend Delivers Advanced, Holistic DDoS Defense

Available today, as part of the A10 Networks solution portfolio, the company has released A10 Defend Detector. A10 Defend Detector provides earlywarning capabilities to facilitate even more effective and advanced threat mitigation, helping customers to build DDoS defenses before attacks occur. A10 Defend Detector, combined with A10 Defend Orchestrator and A10 Defend Mitigator, can provide high levels of scalability and efficacy with automated DDoS defenses for the most demanding service provider and enterprise environments.

A10 is also currently in early trials

A10 NETWORKS HAS THE TRACK-RECORD AND CYBER THREAT EXPERTISE TO HELP CUSTOMERS PROTECT THEIR NETWORKS, EVEN AGAINST PREVIOUSLY UNKNOWN FORMS OF ATTACK. with enterprise customers for its DDoS threat intelligence service, which it plans to integrate into the solution portfolio. A10's security research team already tracks upwards of 15.4 million DDoS weapons globally. The DDoS threat intelligence service builds on that expertise and will provide advanced DDoS intelligence for depth, accuracy, and proactivity. The service will be available early next year.

"A10 Networks has the track-record and cyber threat expertise to help our customers protect their networks, even against previously unknown forms of attack. The launch of our integrated A10 Defend solution portfolio will create the foundation to continue adding new capabilities and supporting new operating environments for customers to achieve optimal user and subscriber experiences," said Dhrupad Trivedi, president and CEO, A10 Networks.

In addition to the A10 Defend solution portfolio, the company can help customers boost web application defenses with the A10 Next-Gen Web Application Firewall, powered by Fastly. Launched earlier this year, A10 is actively working with customers to deploy A10 Next-Gen WAF to help them efficiently and effectively protect their web applications against a wide variety of advanced attacks.

COMMVAULT INTRODUCES FIRST TRUE CLOUD FLATFORM FOR CYBER RESILIENCE

ommvault, a leading provider of cyber resilience and data protection solutions for hybrid cloud organisations, has

announced Commvault Cloud, powered by Metallic AI – a new, unique platform that is changing the game in how IT and security teams can radically improve cyber resilience in an era of non-stop ransomware and malicious cyberattacks.

Commvault Cloud unifies all of the company's SaaS and software offerings on one platform, where visibility and control can be managed holistically via a single pane of glass. But Commvault Cloud goes much further. This new platform is purpose-built for cyber resilience, designed to enable users to predict threats faster, ensure clean recoveries, and accelerate threat response times - all at the lowest possible TCO. And, with Commvault Cloud's unique architecture, customers can secure and recover their data, across any workload, any infrastructure, and from any location to any location.

"Achieving enterprise-grade cyber

resilience is more than building taller walls or deeper moats. It requires a new approach that looks holistically across the entire landscape, from best-in-class data protection and security to Alpowered data intelligence and lightningfast recovery," said Sanjay Mirchandani, President and CEO, Commvault. "With these advanced capabilities and a rich and growing partner ecosystem, our unique and consolidated platform is the new standard in cyber resilience."

With Commvault Cloud users will have access to Arlie – short for "Autonomous Resilience" – a new Al co-pilot that is at their beck and call 24/7 and can respond to inquiries in plain, simple language. But behind the scenes, a lot more is taking place. Arlie will interface with generative Al models that not only consolidate information and reports, but provide users with personalized actionable responses. For example, users may be able to use Arlie to verify or validate a clean point of recovery for critical systems, or generate requested code in seconds.

To begin with, Arlie will integrate on the backend with Azure OpenAI.

Intergrations with other generative AI models will follow soon. Commvault is also announcing AI and security advancements that are coded directly into Commvault Cloud and "show up" as intelligent insights baked into daily workflows.

After a cyberattack, having a clean backup is critical, and so is having a clean location for recovery. That's why Commvault is announcing Cleanroom Recovery. With Commvault Cloud, customers can use this service to recover to a cleanroom in the cloud "at the ready," helping to ensure rapid, frictionless, and reliable recoveries. This offering is great for customers that want to conduct incident response testing on a routine basis.

Commvault is introducing Platinum Resilience, a fully managed service that provides unmatched protection, engagement, and responsiveness to cybersecurity threats and disaster situations. This service, which is being introduced to select customers as part of an early access preview program with full availability planned in early CY 2024. **1**

nínjaOne

The Unified IT Management Platform



Manage, Patch and Support All your Endpoints

- ✓ Unify and automate device management
- ✓ Get 360° visibility and control
- ✓ Patch and support any device anywhere
- ✓ Free onboarding, free training, free support
- ✔ Quick to deploy, easy-to-use, with a single intuitive UI



ninjaone.com

LEARN MORE



ACCELERATE YOUR DIGITAL TRANSFORMATION TO UNLOCK BUSINESS VALUE

YOU CAN COUNT ON US

Rapid advancements in technologies are reshaping industries, fostering new business models, and challenging traditional practices. To thrive in the coming decade, organizations must embrace change, reinvent themselves, accelerate digitization and deliver great customer experience.

At BCT, for over 24 years, we've assisted clients worldwide in unlocking business value from their digital transformation initiatives. Our winning formula comes from our unique combination of innovative IP products, customer-centric IT services, and strategic technology partnerships.



www.bahwancybertek.com