ISSUE 77 | SEPTEMBER 2023

WWW.TAHAWULTECH.COM

ADVISOR

MIDDLE EAST

ANITA JOSEPH CAUGHT UP WITH RANJITH KAIPPADA, MD, CLOUD BOX TECHNOLOGIES, TO FIND OUT HOW THE COMPANY IS PLAYING A PIVOTAL ROLE IN SAFEGUARDING BUSINESSES AGAINST EVOLVING CYBER THREATS AND ENSURING SEAMLESS DIGITAL TRANSFORMATION.

Secural Middle E

🕸 tahawultech.com





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
- Al-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!



CONTENTS









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

18 Ned Baltagi, Managing Director, Middle East, Turkey and Africa at SANS Institute, on how AI is reshaping the cyber skills landscape 26 Rakesh Ragudharan, Vice President, Strategic Initiatives, Bahwan CyberTek, on how a hybrid security approach blends the familiarity of onpremises security with the innovation of the cloud.

42 Gail Coury, SVP and CISO, F5 on how a company's AI strategy should also cover how changes brought about by AI automation will affect employees and customers.



Growing "True" Value-Added **IT Distributor the Middle East** regions with on-the-ground presence in 7 countries

The astest Growing

www.gulfitd.com





EDITOR'S NOTE



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

> Anita Joseph Editor

EVENTS



GUARDIANS OF CYBERSPACE

SECURING

CYBERSPACE

n this era of digital ubiquity, the realm of cybersecurity has evolved into a dynamic battlefield, where new threats emerge with unprecedented speed. As technology advances, so do the methods of malevolent actors seeking to exploit vulnerabilities. It's in this landscape that the Security Operations Center (SOC) emerges as the vigilant guardian, tirelessly monitoring, defending, and orchestrating the defense against an ever-growing

spectrum of cyber threats.

This edition of our security magazine delves deep into the

heart of SOC's significance in safeguarding our digital frontiers. The SOC stands as the beacon of cyber resilience, a hub of technology and expertise that actively detects, analyses, and responds to threats, ensuring the sanctity of our digital assets.

However, the cybersecurity landscape is a tapestry woven with intricate threads of innovation. Beyond the perimeters of traditional defense, we embrace emerging trends that redefine how we combat digital malevolence. From Al-driven threat analysis to the critical role of threat hunting, this issue unpacks the tools and strategies at the forefront of the battle for digital security. In the midst of accelerating digital transformation, our discussions wouldn't be complete without addressing the imperative of collaboration. We spotlight the harmony between SOC, enterprises, and technology partners, illustrating the synergy that elevates our collective cyber defences. It's this collaboration that amplifies our ability to tackle challenges ranging from ransomware to supply chain vulnerabilities.

> As we navigate a future marked by ever-evolving threats, our mission remains unchanged: to empower our readers with the

insights, strategies, and knowledge to not only survive but thrive in the digital age. Together with the unsung heroes within SOC walls and the visionaries forging new security horizons, we strive to bring you a symphony of knowledge that fortifies the digital realm.

Welcome to an edition that not only explores the present and future of cybersecurity but celebrates the indomitable spirit of innovation and vigilance that underscores it. We invite you to immerse yourself in the narratives that illuminate the way forward—because the safeguarding of our digital world rests in our hands. Happy Reading!

Published by

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

SANS INSTITUTE EMPOWERS SAUDI ENTERPRISES WITH SANS RIYADH CYBER LEADERS TRAINING COURSE

SANS Institute, the global leader in

cyber security training and certifications, held its training program SANS Riyadh Cyber Leaders 2023, from August 20 - 24, 2023, at the JW Marriott Hotel Riyadh. In an increasingly complex threat landscape, this intensive course has been designed to empower security leaders in managing risks, creating and leading high-performing security teams and strategising proactively.

Ned Baltagi, Managing Director, Middle East, Turkey and Africa at SANS Institute said, "With the rising frequency and sophistication of cyber threats, creating a culture of cybersecurity awareness within an organisation is crucial. In the event of a cybersecurity breach, leaders must be able to respond quickly and effectively to minimise damage and ensure business continuity.

"Training is essential for developing competent leaders who can protect organisations from cyber threats, manage risks, and align security efforts with business objectives. Understanding risk is vital for making informed decisions on resource allocation and prioritising security initiatives. Moreover, cybersecurity leaders must align security initiatives with broader business objectives and learn how to make decisions that contribute to the overall success of the organisation," Baltagi added.

SANS Riyadh Cyber Leaders 2023 featured two modules led by certified industry experts and practitioners. MGT512: Security Leadership Essentials for Managers, led by Brian Ventura,



taught participants how to effectively communicate complex technical concepts to technical and non-technical stakeholders alike, collaborate with various departments, and appropriately plan and manage security projects and initiatives. Mark Williams led MGT514: Security Strategic Planning, Policy, and Leadership, where leaders were made to understand the tools and skills to bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs.

SENTINELONE STREAMLINES VULNERABILITY MANAGEMENT WITH SINGULARITY RANGER INSIGHTS

Vulnerabilities are on the rise, and

the pressure is on for companies to manage them with greater speed and transparency. To help them do it, SentinelOne, a pioneer and leader in autonomous threat detection and prevention, today announced the launch of Singularity Ranger Insights. Building on the company's top-ranked asset discovery and protection capabilities, the innovative solution removes the complexity from vulnerability management, enabling companies to continuously discover unmanaged assets, evaluate and prioritise threats and mitigate risk using a single console and



agent. The news came during Black Hat 2023, the premier cyber security event being held in Las Vegas recently.

"Today's work-from-anywhere world has opened the door to an increasing number of vulnerabilities, and when it comes to managing them, the stakes have never been higher," said Lana Knop, Vice President of Product Management, Endpoint and Identity Products, SentinelOne. "More than 25 percent of all breaches are the result of vulnerability exploitation, and the average cost of remediating them can top \$4.5 million. With Singularity Ranger Insights, security teams have a powerful tool they can use to reduce the time, cost and complexity of vulnerability management and significantly improve their security posture."

TENABLE INTEGRATES GENERATIVE AI CAPABILITIES WITH LAUNCH OF EXPOSUREAI

Tenable, the Exposure Management

company, has announced the launch of ExposureAI, new generative AI capabilities and services across the Tenable One Exposure Management Platform. Tenable has also introduced Tenable Exposure Graph, a scalable data lake, Powered by Snowflake, that fuels the ExposureAI engine. This unified data platform representing more than 1 trillion unique exposures, IT assets and security findings (vulnerabilities, misconfigurations and identities) across IT, public cloud and OT environments - is the largest repository of contextual exposure data in the world and feeds all of Tenable's Exposure Management products.

Prevention has long been a challenge for security teams. Conducting analysis, interpreting the findings and identifying what steps to take to remediate and reduce risk has traditionally been a time-consuming process that puts organisational security in reactive mode. Nearly six in 10 (58%) cybersecurity and IT pros say the security team is too busy fighting critical incidents to take a preventive approach to reducing their organisation's exposure.1 Furthermore, 73% of cybersecurity and IT pros believe their organisation would be more successful at defending against cyberattacks if they could devote more resources to preventive cybersecurity.2

Harnessing AI efficiently requires data and expertise to generate meaningful insights. Since the introduction of its dynamic Vulnerability Priority Rating (VPR) in 2019, Tenable has applied AI techniques to help organisations prioritise vulnerabilities based on true risk to the business. Recently, Tenable Research made generative AI-developed research tools available for free to the



cybersecurity community. Now Tenable is using generative AI to put more power than ever in the hands of security teams, so they can be more efficient and focus more resources on preventing successful attacks. The insights Tenable ExposureAI creates make exposure management more accessible and turn all analysts into expert defenders.

CLOUDFLARE BOT MANAGEMENT NOW ON IBM CLOUD INTERNET SERVICES TO ADDRESS GROWING THREAT LANDSCAPE FOR ENTERPRISES

Cloudflare, Inc. the security,

performance, and reliability company helping to build a better Internet, has announced that IBM Cloud Internet Services (CIS), powered by Cloudflare, has expanded its offering to include Cloudflare Bot Management, now available to help enterprises on the Enterprise Premier Plan address and combat the growing threat of malicious bot traffic.

Cloudflare and IBM Cloud have been working together since 2018, integrating Cloudflare application security and performance natively into IBM Cloud through IBM CIS, powered by Cloudflare. CIS positions customers to configure their web and Internet applications to be



protected against cyber threats including DDoS attacks and data theft, while enhancing performance and reliability with load balancing, optimised routing and caching, and data exchange, as part of the CIS suite of capabilities.

As malicious bot attacks become more sophisticated and manual mitigations become more burdensome, a dynamic and adaptive solution is required for enterprises running Internetfacing workloads. With Cloudflare Bot Management, businesses can be protected from targeted application abuse such as credential stuffing, inventory hoarding, carding abuse, and content scraping, as part of the complete Bot Management detection and mitigation offering. The Cloudflare Bot Management feature is available now for any IBM Cloud CIS customer with an Enterprise Premier Plan.

BEYONDTRUST'S IDENTITY SECURITY INSIGHTS PROVIDE UNPRECEDENTED VISIBILITY INTO IDENTITY THREATS

BeyondTrust, the worldwide leader in

intelligent identity and access security, has announced the general availability of its groundbreaking Identity Security Insights solution. With the escalating complexity of cyber threats targeting identities and credentials, this innovative solution sets a new standard in securing both human and non-human identities and privileges, providing organisations with unparalleled visibility and advanced identity-first threat detection capabilities.

Identity Security Insights represents a transformative addition to the BeyondTrust platform, providing an advanced intelligence layer that empowers organisations to achieve new levels of identity and access security. The solution offers a unified view of identities, accounts, cloud entitlements, and privileged access across the entire identity estate, enabling organisations to seamlessly correlate data from both BeyondTrust's products and third-party identity providers, such as Okta, Ping Identity, and Microsoft Entra ID (formerly Azure AD), and cloud providers, such as AWS and Azure.

"Identity Security Insights completely revolutionises the way organisations approach identity security, providing an unprecedented level of visibility, threat detection, and actionable insights that haven't been available to date," said



Marc Maiffret, CTO of BeyondTrust. "We focus on securing the privileges and access that make compromised identities dangerous. By empowering organisations to proactively protect their identities, we're continuing to spearhead advancements in cybersecurity that safeguard critical assets in today's evolving threat landscape."

VMWARE CARBON BLACK LAUNCHES THREAT DETECTION AND RESPONSE FOR MODERN APPLICATIONS

VMware, Inc. has announced

advancements in its Carbon Black Extended Detection and Response (XDR) strategy focused on cloud native applications. Cloud Native Detection and Response (CNDR) provides VMware Carbon Black customers with unified visibility, security, and control in highly dynamic and complex modern application environments.

Containers and Kubernetes have become synonymous with the modern application transformation as organisations increasingly adopt multi-cloud and hybrid technology infrastructures. However, the growth in cloud native architectures and containers also expands an organisation's attack surface. As Security Operations Center (SOC) teams are tasked with learning the complexities of cloud native environments, they also are challenged with containers running in production



with limited-to-no security coverage, disparate tools that create gaps in coverage, and limited visibility into the different layers of these applications.

VMware Carbon Black's new CNDR capabilities expand its leading XDR solution and are designed to deliver enhanced threat detection for containers and Kubernetes within a single, unified platform. These enhancements aim to deliver runtime protection for Linux containers to provide a scalable approach for protecting applications from emerging threats and helping eliminate blind spots for attackers to exploit.

"The rise of containers, and often the resulting lack of visibility and limited control security teams have, has created a perfect storm for attackers to target cloud native applications as a means of entry into an enterprise," said Jason Rolleston, vice president and general manager of VMware Carbon Black. "In order for security teams to keep up, it's critical that organisations have security visibility and control that spans the entire application lifecycle and does not require them to be experts in containers and Kubernetes. With our advanced CNDR solution, VMware Carbon Black is the only partner that delivers threat detection and response from a single console across endpoints, workloads, and containers."

Solar Powered Camera

No network cable required

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

Easy installation

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

Can withstand bad weather

Prone to extreme weather such as strong wind and rainstorms.



40W



20 Ah lithium

4G





Scan to Learn More

HIKVISIONMENA in HIKVISION-MENA

O HIKVISIONMENA HIKVISIONMENA



FRANK LEYMANN NAMED FIRST WS02 TECHNOLOGY FELLOW

SO2, the leader in digital transformation technology, has announced that Prof. Dr. Frank Leymann has been named the first WSO2 Technology Fellow, the highest technical rank in the company. The title recognises the global impact that Frank has made through his technical innovations and leadership in working with WSO2, software industry groups, governments, and universities, among others. To date, Frank has earned 43,000-plus technical citations, and he is the co-author of more than 500 peer-reviewed papers, some 70 patents, and several industry standards.

The WSO2 Technology Fellows

Program was introduced in 2023 to honor individuals who have not only made exceptional technical contributions to WSO2 but also have earned recognition as a global-scale authority in a technical field of practice. Honorees are appointed by a committee of peers within WSO2 that includes the CEO, senior technical executives, and any current Technology Fellows.

"I have had the privilege of knowing Frank since we first began collaborating on web services standards in 1999. His contributions to software standards have helped to fundamentally change the way organisations create, integrate and deliver applications," said Dr. Sanjiva Weerawarana, WSO2 founder and CEO.



"Frank has also played a strategic role in evolving our own software for developing and delivering digital experiences. As our first Technology Fellow, he is an exceptional candidate without parallel in WS02."

Prior to becoming a WS02 Technology Fellow, Frank Leymann served as a consultant architect at WS02 for nearly a decade. Additionally, Frank has been a full professor of computer science at the University of Stuttgart, Germany since 2004, where he is also the founder and director of the Institute of Architecture of Application Systems. His research interests include middleware, cloud computing and associated systems management aspects, quantum computing, and pattern languages.

Prior to joining the university, Frank served in software development roles at IBM for two decades where he was appointed an IBM distinguished engineer and became an elected member of the IBM Academy of Technology. During his tenure at IBM, he contributed to software products, such as DB2, WebSphere and the MQSeries. Frank also was the main co-inventor and chief software architect of IBM's business process management and workflow products.

Frank has been recognised for his technical contributions by leading technical, scientific, academic and government organisations: He is an elected member of the Academy of Europe, as well as a fellow at both the Asia-Pacific Artificial Intelligence Association (AAIA) and Center of Integrated Quantum Science and Technology (IQST). He also earned appointments as a member of the Expert Council for Quantum Computing of the German Government and a Kurt Gödel visiting professor for Quantum Computing, TU Wien.







12TH SEPTEMBER 2023 TAJ EXOTICA RESORT & SPA, THE PALM, DUBAI

CPI Media Group and **tahawultech.com** would like to sincerely extend our thanks to all our sponsors for the **CISO 50 & Future Security Awards 2023**. Your unwavering support helped make the awards a HUGE success.

Thank You Sponsors

CLOUD PARTNER

SOLARWINDS

GOLD SPONSORS

Barracuda. LINKSHADØW

INFOSEC THALES In Pursuit of Excellence Building a future we can all trust





SILVER SPONSOR

CYBERHUB 24x7 CSOC

#CISO50FSA2023 | #tahawultech



CATALYST OF CHANGE

ANITA JOSEPH CAUGHT UP WITH **RANJITH KAIPPADA,** MD, CLOUD BOX TECHNOLOGIES, TO FIND OUT HOW THE COMPANY IS PLAYING A PIVOTAL ROLE IN SAFEGUARDING BUSINESSES AGAINST EVOLVING CYBER THREATS AND ENSURING SEAMLESS DIGITAL TRANSFORMATION.

ould you provide an overview of the comprehensive solutions portfolio offered by Cloud Box Technologies and how the company contributes to the smooth and seamless digital transformation journey of businesses?

In recent years, the surge in digital transformation has been palpable across various industries in the UAE. Companies are increasingly recognising the value of this shift and the associated business benefits that it brings. However, this journey is not without its challenges. In fact, there are many uncertainties surrounding digital transformation, often overlooked or misunderstood by people. However, these uncertainties must be openly discussed and effectively addressed to ensure its successful implementation and resolution.

Amid the buzz surrounding digital transformation, Cloud Box Technologies

(CBT) steps in as an expert consultant, guiding businesses through a step-bystep progression in this transformative process. Recognising that each customer's journey is unique, CBT tailors its solutions to the specific needs of each client, capitalising on digital technologies to elevate businesses to the next level.

Since every customer has a unique profile, it makes it impossible to standardise digital transformation technology or processes across all companies. Therefore, it is imperative to base our approach on understanding each customer's experience and focus on the key areas where digital transformation can make an impact. At CBT, we analyse the various digital technologies that can elevate businesses to the next level, acting as a catalyst for this progression. For instance, the requirements for a hospital will differ from those of a retail business or the banking sector. Precisely comprehending each customer's needs is a fundamental step.

Investing in data and analytics is a significant undertaking, albeit expensive, and while the market offers numerous reporting and data analytic tools, the question of investment readiness arises. As a System Integrator, we firmly believe in the necessity of these tools to drive transformation. Guiding customers towards the right product and tool selection, as well as effectively consolidating and deriving valuable insights from data, is a key service we provide.

Stepping into the realm of technology, we leverage our expertise to guide customers through the adoption of new technologies. Our approach varies based on the specific industry, be it healthcare, banking, or others. While our uniqueness lies in our market approach, success hinges on effective consultation and providing accurate information to customers. Our role is to understand industries, recommend the most suitable technologies for business profitability and cost reduction, and guide customers seamlessly through the whole process.

In short, as the momentum behind digital transformation grows, CBT acts as an advocate for customers, providing expert guidance that ensures a smooth and purposeful digital transformation. Instead of offering standardised

OUR SOC SERVICE OFFERS A COMPREHENSIVE APPROACH TO → CYBERSECURITY THAT COMBINES ADVANCED TECHNOLOGY WITH HUMAN EXPERTISE.

AT CBT, WE ANALYSE THE VARIOUS DIGITAL \rightarrow TECHNOLOGIES THAT CAN ELEVATE BUSINESSES TO THE NEXT LEVEL, ACTING AS A CATALYST FOR THIS PROGRESSION.

solutions, CBT pinpoints core areas where transformation is required based on each customer's unique experience and objectives.

For digital transformation to be seamless, there needs to be the right set of skills. Do you think there is enough skilled workforce out there today to meet the demand for new technology implementation? How does Cloud Box Technologies address the scarcity of skilled professionals? The shortage of skilled professionals is a pressing issue in today's market. Convincing CEOs and investors of the

importance of technology adoption can be

challenging, as the understanding of its implications often varies between C-level executives and the general workforce. Bridging this gap requires a bottom-up approach, where employees across all levels comprehend the significance of digital transformation. CBT recognises this necessity and employs a specialised team of skilled engineers who possess the expertise to understand customer needs and effectively facilitate the transformation. We ensure that the right skill sets are in place to guide clients through successful digital transitions.

We step in as a specialised technology partner, differentiating ourselves from other resellers by being a Value-Added



Service Provider. Our focus is sharp - we select specific verticals, and at present, our strength lies in the healthcare sector, along with hospitality and retail industries. CBT excels in identifying gaps within individual verticals, enabling us to pinpoint the necessary skill sets to address specific needs. Our team consists primarily of technically skilled engineers who adeptly grasp customer requirements and provide the right solutions. Our current success is underscored by the simultaneous management of nearly a dozen products, ensuring that our experts are strategically positioned to guide





customers through a successful digital transformation. This track record of accomplishment has led to an increasing trust in our capabilities year after year.

Can you elaborate on the significance of Security Operations Centers (SOCs) in today's landscape and how CBT contributes to securing businesses against advanced cyber threats?

Digital transformation is not an isolated activity. It is not just enough to implement extensive technological changes, safeguarding these investments also becomes paramount. Security Operations Centers (SOCs) play a pivotal role in this aspect, and CBT's SOC provides round-the-clock monitoring and support, ensuring that no cyberattacks compromise a business's digital infrastructure. While many SOCs merely detect threats, CBT's SOC goes further by enabling instant response and recovery.

Our SOC service offers a comprehensive approach to cybersecurity that combines advanced technology with human expertise. Our team is equipped with the latest tools and technologies to detect and respond to cyber threats in real-time. We also have a deep understanding of the threat landscape and can anticipate new attack vectors

The CBT SOC will support customers with the following

Continuous Protection - 24/7 uninterrupted monitoring of network to detect potential threats.

Security Intelligence - Using the latest tools to identify and mitigate cyber threats in real-time.

Quick and Effective Risk Management -Comprehensive approach of advanced technology with human expertise helps detect threats and respond and mitigate risks quickly.

Threat prevention - Deep understanding of the threat landscape helps in providing potential view of the network anticipate new attack vectors even before they emerge.

Proactive incident response strategies - Proactive detection and response to threats in real-time reduce risk of data breach or cyber-attacks and help identify any potential weaknesses that can be exploited.

Cost Savings - The latest security solutions to help stay ahead of cyber threats and damage, thus saving potential costs incurred due to the security breaches.

Regulatory Compliance - Regulatory compliance such as HIPPA and GDPR and regular compliance reports.

before they even emerge. This holistic approach safeguards against data loss and ensures rapid recovery in the event of an attack, setting us apart in the market.

Our SOC service can also help you meet regulatory compliance requirements. Many industries are subject to strict data protection regulations, such as HIPAA and GDPR. Failure to comply with these regulations can result in hefty fines and legal penalties. Our SOC service can help you stay compliant by monitoring your systems for any potential violations and providing you with regular compliance reports.

How is SOC expected to help CBT, particularly with its future growth plans?

Cyberattacks and cybersecurity are here to stay, just as we anticipate virus attacks and counteract them with antivirus solutions. The prevalence of widespread cyber-attacks and security breaches is undeniable, but defending against this onslaught is the challenge. Although multiple Security Operations Centers (SOCs) exist, not all offer round-the-clock protection within the UAE. Many rely on foreign operations and manpower, lacking local presence. This is precisely where CBT takes the lead. We're making substantial investments in a 100% local SOC. based in the UAE, ensuring continuous monitoring of potential threats. Our skilled team of engineers, well-versed in SOC dynamics, local intricacies, and cutting-edge technology, provides end-to-end support. This commitment differentiates us from competition; we're here to demonstrate unwavering support to our customers at every step.





We all know that the future is unpredictable, with rapid technological advancements and ever-growing cyber threat-attack vectors. So, what is CBT's go-to market strategy going to be, for the GCC market in particular?

CBT's strategy revolves around teamwork, collaboration, and differentiation. Rather than serving as a mere intermediary, CBT positions itself as a digital transformation enabler. By bridging the gap between vendors and customers, CBT ensures that technology messages are effectively translated and implemented. This unique approach has earned CBT a reputation as a premium cluster System Integrator, with

$\begin{array}{l} \text{OUR ROLE IS TO UNDERSTAND INDUSTRIES AND} \\ \rightarrow \text{RECOMMEND THE MOST SUITABLE TECHNOLOGIES} \\ \text{FOR BUSINESS PROFITABILITY AND COST} \\ \text{REDUCTION.} \end{array}$

a focus on both quality and relevance. With the addition of a local SOC, CBT plans to enhance customer trust and accelerate business growth, eventually expanding its presence to neighboring countries.

To sum up, Cloud Box Technologies stands out as a guiding force in the ever-evolving landscape of digital transformation, ensuring that businesses navigate this journey with expertise and confidence. By tailoring solutions, addressing skill shortages, bolstering cybersecurity, and fostering collaboration, CBT remains at the forefront of driving impactful change across industries.

BRIDGING THE AI-SECURITY GAP

ANITA JOSEPH CAUGHT UP WITH **NED BALTAGI**, MANAGING DIRECTOR, MIDDLE EAST, TURKEY AND AFRICA AT SANS INSTITUTE, TO DISCUSS HOW AI IS RESHAPING THE CYBER SKILLS LANDSCAPE.

s AI continues to advance, its applications in cybersecurity are becoming more prominent. Can you discuss some of the latest trends and opportunities you see at the intersection of AI and cybersecurity, and how SANS Institute is positioning itself to address these developments? SANS has been leading the intersection between AI and cybersecurity for several years now. As the nexus between AI and cybersecurity grows tighter, we're witnessing transformative changes in threat detection, response strategies, and predictive analytics. The cybersecurity landscape is becoming increasingly dynamic, with threats evolving in complexity almost daily. Al's capability to rapidly analyse vast datasets, recognise patterns, and predict future threats is revolutionising the approach to cybersecurity.

SEC595: Applied AI and Machine Learning for Cybersecurity Professionals continues to be the only publicly available class that teaches cybersecurity professionals how AI and machine learning work, how to think about security problems in a way that allows them to be solved using AI solutions, and teaches professionals how to build AI solutions using both traditional statistical and probabilistic learning in addition to neural networks. To be sure, the field is advancing. We continue to see that vendors are more focused on being able to claim that a tool uses AI or has AI capabilities, but the reality is that the features currently available remain limited. More often than not, it continues to be necessary to extract or duplicate log and other data to an AI/ML pipeline to be able to perform powerful automated analysis since the capabilities within the SIEM tools, for example, are so limited.

With the growing complexity of cyberattacks, skill gaps in the cybersecurity workforce have become more apparent. How does SANS Institute contribute to closing these gaps by equipping professionals with the necessary skills to defend against AI-driven attacks and vulnerabilities?

Defending against AI attacks is really no different than defending against previous attacks. The only real difference is the ability to leverage AI to mutate humanbased attacks much more quickly and to do so even if the attacker is not fluent in the language of the victim. SANS continues to be the most trusted and best source of practical "How To" information for securing and managing security in an enterprise.

As for vulnerabilities introduced by AI systems, the answer is also yes. We fully prepare professionals to not only understand, use, and create these systems, it also makes them intimately familiar with the risks and vulnerabilities

SANS INSTITUTE IS UNDENIABLY PAVING THE WAY FOR A FUTURE WHERE → AI AND CYBERSECURITY ARE SEAMLESSLY AND EFFECTIVELY INTERTWINED.

SPOTLIGHT / SANS INSTITUTE

of such systems. As the field evolves, additional risks are coming to the fore. For example, a major risk today that enterprises are not adequately aware of involves the use of the various AI APIs.

Collaboration between human experts and AI systems is key to effective cybersecurity. How does SANS Institute emphasise the importance of human-AI collaboration in its training, and how do you prepare students to make informed decisions in high-pressure cybersecurity scenarios?

This is a very important question. AI/ML really is not at a state in cybersecurity where it could realistically be used to replace humans. It's not even close. Too many vendors are positioning their products in a way that effectively claims that once the AI system is in place, humans need not ever worry about the problem again. This simply isn't true and creates risk!

AI and ML systems, when built properly, allow cybersecurity professionals to manage vast amounts of data with limited resources. When built carefully, these systems allow the AI systems to do everything the AI systems are good at and free the humans to do tasks that humans are great at, but AI systems are not.

As a specific example, we build a system with students in SEC595 to identify unusual application protocols in use on a network in real-time. While a human can perform this task, there is no practical way for them to do it in realtime. In fact, given the amount of data passing through a network on any given day, it would take a massive effort to sift through these connections to identify unusual application protocols within the data. (In case your readers are thinking, "Just look at the port numbers," we're talking about the application protocol running over the TCP or UDP session



regardless of the port number in use.). So, we build and train an extremely effective AI that can solve this problem in real-time – but just because the AI finds something unusual does not mean that it is bad. That's where the human comes in. The AI can raise an alert, perhaps to the SIEM, sending the communication to a human expert for a final determination.

Preparing students for high-stress situations is crucial. We simulate realworld cybersecurity breaches where AI tools provide real-time insights, and students must make swift decisions to mitigate threats. Through repeated exposure to such scenarios, students develop the poise and decisiveness needed to handle actual cybersecurity crises. We emphasise the importance of trusting AI-driven data while also applying critical human judgment to make the best possible decisions in highpressure environments.

As AI technology evolves, new security challenges will inevitably arise. How does SANS Institute foster a culture of continuous learning among its students and alumni, encouraging them to stay updated on AI-related security developments throughout their careers? The SANS Institute recognises the rapidly shifting landscape of AI and its profound implications for cybersecurity. To ensure our students and alumni are always at the cutting edge, we make it

THE SANS INSTITUTE RECOGNISES THE RAPIDLY \rightarrow SHIFTING LANDSCAPE OF AI AND ITS PROFOUND IMPLICATIONS FOR CYBERSECURITY.



a priority to frequently update courses, like the pivotal SEC595, to mirror the latest in AI methodologies and threat vectors. Beyond formal coursework, our robust alumni networks and online platforms act as crucibles for knowledge exchange, facilitating discussions on emerging threats and technologies. Through a blend of specialised event workshops, webinars, and real-world cybersecurity challenges centered around AI, we foster an environment of continuous learning, keeping our community informed, engaged, and realworld ready.

In the intricate tapestry of AI and cybersecurity, the SANS Institute serves as a crucial thread weaving together innovative training and research to prepare the broader security team for imminent challenges. While specialists equipped with knowledge from courses like SEC595 are central to AI integration, SANS recognises the imperative need to ensure that the entire security team is AI-literate. By instilling foundational AI concepts across its spectrum of courses, we ensure that all members can effectively interface with AI tools, harnessing them to detect and respond to threats.

The SANS Institute's continuous engagement with industry stakeholders and research reflects its commitment to driving the AI-cybersecurity nexus forward. Fresh insights and evolving AI techniques are promptly integrated into training curriculums. As a result, security teams aren't just passive recipients of AI innovations but active contributors, shaping AI's future role in cybersecurity. By championing continuous learning, fostering interdisciplinary collaboration, and emphasising the synergy between human expertise and AI capabilities, the SANS Institute is undeniably paving the way for a future where AI and cybersecurity are seamlessly and effectively intertwined.

How would you summarise the unique value proposition that SANS Institute offers to individuals seeking to enhance their expertise in AI and cybersecurity, particularly in navigating the complex security considerations in the age of AI?

The SANS Institute is uniquely positioned at the crossroads of AI and cybersecurity, setting the trajectory for the evolving fusion of these fields. One of our undeniable strengths lies in our instructors – all seasoned professionals actively engaged in the sector. Each course, including SEC595, isn't merely theoretical; it's enriched with the firsthand experiences and insights of these industry experts.

These instructors don't just teach; they bring real-world challenges to the classroom, bridging the gap between academic learning and practical application. By integrating their current, on-the-ground experiences with cuttingedge research, SANS ensures that students are not only well-prepared for today's AI cybersecurity challenges but are also equipped to shape its future. We offer the only practical course in AI and ML for cybersecurity professionals that teaches them everything they need to know to create effective threat-hunting and other cybersecurity tools using statistical, probabilistic, and neural network techniques. The students do not learn how to use a certain vendor's interface but instead, learn how AI really works and are capable of building solutions using any vendor's environment.

In essence, SANS offers professionals an unmatched opportunity to learn from the best in the business and to be pioneers in the AI cybersecurity landscape.

HIKVISION UNVEILS NEW SMART MANAGED SWITCHES FOR MANAGING SECURITY SYSTEMS REMOTELY

HIKVISION LAUNCHED A NEW GENERATION OF SMART MANAGED SWITCHES THAT, IN CONJUNCTION WITH THE HIK-PARTNER PRO MOBILE APP, ENABLE INSTALLERS TO REMOTELY DEPLOY AND CONFIGURE SECURITY SYSTEMS WITH COMPREHENSIVE OPERATION AND MAINTENANCE CAPABILITIES. THIS NEW GENERATION OF SMART MANAGED SWITCHES FEATURES A ROBUST ARCHITECTURE WITH 6 KV SURGE PROTECTION FOR POE PORTS. THE FULL PORTFOLIO RANGES FROM AN ECONOMICAL 100 MBPS SWITCHES UP TO HIGH-POWERED GIGABIT SWITCHES TAILORED FOR SMB PROJECTS.

eamless integration with security systems

A rapid increase in the number of IP devices needed to fit the wide varieties of security scenarios has made network switches an essential tool. However, while traditional plug-and-play network switches provide connectivity, they may not converge with other security devices to extend synergy within a system. As the network in a business scenario becomes more complex, the device configuration becomes cumbersome and actually increases the workload.

But now, with this new generation of Smart Managed Switches, Hikvision integrates connectivity with management over the entire security system through its mobile app, Hik-Partner Pro. Hik-Partner Pro weaves together cameras, alarms, NVRs, access control devices, and software, creating a unified and easyto-use security system for centralized, visualized operations and maintenance.

Further, with the mobile Hik-Partner Pro app, entire system deployment and configuration can be completed with a mobile phone in just three steps, making delivery simpler, faster and easier. The seamless integration provides installers with an all-in-one experience. Here's more on how it works.

Remote management – just like being on-site

The new generation of Smart Managed Switches enables installers to implement network operations and maintenance remotely, with no need to be at the site they are servicing. Two elements are critical here for maintaining such a



setup: an intuitive bird's-eye-view of the system as well as a way to resolve issues that come up.

- Visualised network topology. A network topology, visualised in the mobile app, allows installers to view and maintain a network intuitively, easily getting updates on network health status and device connection status.
- Efficient troubleshooting. Installers get real-time alarm notifications when

a network or a device goes down, helping them quickly and remotely locate and resolve issues ranging from port reboots to parameter adjustments and more. This significantly reduces system downtime, as well as network operations and maintenance costs.

Doing more in less time with lower expenditure

Remote management saves time and eliminates transportation costs for installers. With Hik-Partner Pro, installers will extend and elevate their work efficiency as they maintain products using a mobile phone from any location and at any time of day, responding more quickly to ensure stable system performance for their customers. It can be a powerful tool for expanding their business and satisfying their customer base.

To discover more about Hikvision's Smart Managed Switches and how they support remote configuration and management of an entire security system while combining functionality, simplicity and performance, please visit the Hikvision product page.

VERITAS NAMED A LEADER IN THE 2023 GARTNER MAGIC QUADRANT FOR ENTERPRISE BACKUP AND RECOVERY SOFTWARE SOLUTIONS

eritas Technologies, the leader in secure multi-cloud data management, has been positioned as a Leader in the Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions (EBRSS). Veritas is the only vendor that Gartner has named a Leader in each of its last 18 enterprise backup and recovery software reports.

A trusted partner of 95% of the Fortune 100, Veritas remains at the forefront of innovation in data protection, application resiliency and data compliance and governance. Having supported enterprises throughout every major IT transition, Veritas is helping organisations navigate a new world – where data lives across environments, cyberthreats loom, cloud costs and regulatory fines are rising, and organisations often lack the in-house technical expertise to address these complexities.

Lawrence Wong, senior vice president

and chief strategy officer at Veritas, said: "Veritas has an unparalleled track record of persistent innovation aimed at resolving our customers' data resiliency challenges. Throughout this journey, Gartner has consistently recognised us as a leader in its enterprise backup and recovery software solution Magic Quadrant reports. Today, businesses face unprecedented cyber threats to their increasingly heterogeneous cloud environments. We believe that our position in the 2023 Gartner Magic Quadrant for EBRSS reflects our ability to counter those threats with the industry's most comprehensive portfolio of cloudnative cyber recovery solutions."

Veritas believes that it is recognised in the Gartner Enterprise Backup and Recovery Software Solutions Magic Quadrant because of these three key areas:

• Veritas Alta – A secure, unified and cloud-native data management platform that brings together a



broad array of enterprise-class data services. The platform features data protection with unmatched ransomware resiliency and enables customers to manage their entire data protection estate via the Alta View single-pane-of-glass console. Veritas Alta also provides the highest levels of application resiliency, application portability across clouds and optimisation of storage consumption. Veritas Alta additionally allows enterprises to illuminate and remediate information risks with data compliance as-a-Service.

- Cloud Scale Technology A secure, next-generation architecture designed to operate natively in the cloud, Cloud Scale Technology powers a containerised, elastic and Al-based microservices architecture that provides unified data management services across any cloud. Cloud Scale Technology helps enterprises improve operational agility, data security and efficiency, while also achieving cost savings in multi-cloud environments.
- Autonomous Data Management (ADM) – With Cloud Scale Technology serving as the foundation, Veritas has outlined a product vision to transform the future of data management and empower enterprises to regain control over their data through ADM. This groundbreaking approach leverages automation and AI/ML technologies to dramatically reduce operational complexity. The shift from manual processes to ADM-led self-optimising, self-healing and self-provisioning will redefine data protection and recovery in the age of multi-cloud and beyond. 1



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.



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

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

THE HYBRID APPROACH RAKESH RAGUDHARAN, VICE PRESIDENT, STRATEGIC INITIATIVES,

RAKESH RAGUDHARAN, VICE PRESIDENT, STRATEGIC INITIATIVES, BAHWAN CYBERTEK, ON HOW A HYBRID SECURITY APPROACH BLENDS THE FAMILIARITY OF ON-PREMISES SECURITY WITH THE INNOVATION OF THE CLOUD.

ow has the traditional approach to cybersecurity evolved in recent years, and what factors have driven the need for a hybrid security approach?

The rapid pace of digital transformation has been a pivotal-point for the cybersecurity landscape and this transformation has brought about the emergence of a hybrid security approach. As businesses increasingly adopt cloud services, IoT devices, and mobile technologies, the traditional perimeterbased security model has become less effective. The perimeter is no longer confined to physical boundaries; it's everywhere these technologies touch. This has led to a realisation that a solely perimeter-centric approach leaves vulnerabilities that can be exploited by cyber adversaries. Besides, the rise in sophisticated cyber threats has prompted organisations to adopt a more dynamic and adaptable stance. Traditional security measures often struggled to keep up with the evolving tactics of threat actors.

The frequency and complexity of attacks like ransomware, zero-day exploits, and advanced persistent threats have pushed businesses to seek a more versatile strategy that can swiftly



respond to changing threat landscapes. A cyberattack occurs roughly every 39 seconds with cybercrime rates having increased by 300% since the COVID-19 pandemic. According to Cybersecurity Ventures, the cost of cybercrime is predicted to hit \$8 trillion in 2023 and will grow to \$10.5 trillion by 2025.

The concept of a hybrid security approach emerges from the need to bridge the gap between prevention and detection. It's all about combining proactive measures with robust detection and response capabilities. This strategy involves not only fortifying the perimeter with firewalls and intrusion prevention systems, but also integrating advanced threat intelligence, behavior analytics, and Al-driven anomaly detection, to identify unusual activities within the network. The modern workforce's inclination towards remote and mobile work has added another layer of complexity. With employees accessing company resources from various locations and devices, a one-size-fits-all security approach no longer suffices. A hybrid model recognises the importance of securing data and applications regardless of their location or the devices used to access them.

Bahwan CyberTek (BCT) understands this reality extensively. Leveraging our expertise in product engineering, we have developed an advanced Managed Security Services and Threat Intelligence Platform. This platform not only addresses present-day threats but also empowers organisations to proactively outpace cybercriminals. Through its robust implementation of 'intelligent threat hunting and investigation' coupled with automated incident response, we enable businesses to maintain security stride-for-stride with the ever-changing landscape of cybercrime. This guarantees their safety and future readiness. In essence, the hybrid security approach acknowledges that while preventing threats is crucial, it's equally vital to swiftly detect and respond to any breach that does occur. It's about creating a resilient cybersecurity ecosystem that

can adapt to evolving threats and provide a multi-faceted defense.

In what ways does a hybrid security approach leverage both on-premises and cloud-based solutions to enhance overall protection?

A hybrid security approach is like the best of both worlds in the realm of cybersecurity. At BCT, we firmly believe in the power of combining on-premises and cloud-based solutions to create a robust shield against evolving cyber threats. Think of it as a dynamic dance between two partners – your on-premises infrastructure and the cloud.

On-premises solutions provide that tangible. localised control over sensitive data and critical applications. They are the stalwarts guarding your castle walls. You're in charge here, and that sense of ownership can be reassuring, especially for highly regulated industries. On the other hand, cloud-based solutions bring an agility that's hard to match. The cloud offers unparalleled scalability and accessibility. It's like having additional reinforcements that can adapt to different threat scenarios. This flexibility is a game-changer, especially in today's landscape where the perimeter of your network is constantly shifting.

So, how does this hybrid dance play out? Imagine a scenario where sensitive customer data resides within your on-premises database, but the processing and analysis of that data happen in the cloud. This way, you're minimising exposure while still enjoying the computational muscle of the cloud. Additionally, a hybrid approach allows you to cherry-pick the best security tools from both worlds. You can leverage your triedand-true on-premises solutions, while also tapping into the specialised expertise of cloud providers. The key is in seamless orchestration between your on-premises and cloud security measures. This often involves robust identity and access management, encrypted communication channels, and continuous monitoring to detect any odd moves on the dance floor.

In a nutshell, a hybrid security approach blends the familiarity of on-premises security with the innovation of the cloud. It's about adapting to the ever-changing threat landscape while maintaining control over your most critical assets.

Can you provide examples of industries or sectors where a hybrid security approach has proven to be particularly effective? What lessons can other sectors learn from these examples?

Absolutely. What's really compelling about the hybrid security approach is its adaptability to various scenarios. which truly emphasises its significance in tackling diverse security challenges. One sector that stands out is the financial industry. Financial institutions have successfully implemented a hybrid security model that combines traditional perimeter defenses with advanced analytics and AI-driven threat detection. By doing so, they've managed to reinforce their networks against both known and emerging threats. This approach allows them to safeguard sensitive customer data while also staying agile in the face of rapidly evolving cyber threats.

Another sector that has embraced the hybrid security approach is healthcare. The healthcare industry deals with a vast amount of sensitive patient information, making it an attractive target for cybercriminals. By integrating robust perimeter defenses with user behavior analytics and real-time monitoring, healthcare organisations can proactively identify and respond to potential breaches. This not only protects patient data but also ensures the continuous availability of critical medical services.

Based on lessons learnt from these and other industries, BCT would suggest that it is essential to acknowledge there is no singular security solution that acts as a perfect remedy. Achieving a complete security stance involves blending various technologies, procedures, and human proficiency. Even though conventional security elements such as firewalls and antivirus programs hold significant

Q&A / **BAHWAN CYBERTEK**

importance, they must be enhanced by state-of-the-art innovations like AI and machine learning. These advanced technologies serve anomaly identification and predictive analysis purposes. The collaboration among IT groups, security professionals, and business divisions is of utmost significance. Particularly within the financial and healthcare domains, this collaboration has facilitated the attainment of a more thorough grasp of the threat environment, leading to the formulation of tailored security approaches.

It is also important to note that continuous improvement and adaptability is key. Cyber threats are dynamic and ever-evolving, so an effective hybrid security approach should be flexible enough to adjust to new attack vectors and vulnerabilities as they arise. Regular assessments, penetration testing, and staying updated on the latest threat intelligence are essential practices.

From our experience and multiple industry examples, there are several key takeaways that other sectors can benefit from:

- **Customisation:** Tailor your hybrid approach to your sector's unique security requirements, data sensitivity, and compliance needs. There's no universal solution.
- **Balance:** Strike the right equilibrium between on-premises control and cloud-based innovation. Different functions have varying needs.
- Data Classification: Clearly categorise data based on sensitivity and regulatory mandates. Decide what data belongs in the cloud and what should remain on-premises.
- **Collaboration:** Foster collaboration between on-premises and cloud security teams. A cohesive strategy amplifies overall security efforts.
- Continuous Monitoring and

Response: Embed continuous monitoring and incident response capabilities across both environments to ensure swift threat identification and mitigation.

 Holistic Approach: Approach security holistically, considering digital assets as well as physical infrastructure. Comprehensive security covers the entire ecosystem.

Some argue that a hybrid security approach could lead to increased complexity. How can organizations manage this complexity while maintaining a strong security posture?

This is a pertinent question, and I appreciate the opportunity to shed some light on it. First off, it's crucial to acknowledge that a hybrid environment inherently introduces a certain level of complexity due to the coexistence of diverse infrastructures. But complexity doesn't have to equate to vulnerability. In fact, with the right strategies in place, it can lead to enhanced security resilience. One of the keystones here is centralised visibility and control. Organisations should invest in robust security management tools that offer a unified view of their entire environment, whether it's in the cloud, on-premises, or somewhere in between. This centralised approach allows security teams to detect threats, monitor activities, and enforce policies consistently across the board. It's like having a single pair of eyes that can spot any suspicious activity, regardless of where it occurs.

Additionally, automation and orchestration play pivotal roles in simplifying complex security tasks. This has been incredibly showcased by our Threat Intelligence Planform, which integrates big data analytics, intelligent threat hunting, threat incident investigations, automated incident response, and user experience behavioural analysis (UEBA). It is a vital tool

THE GOAL IS TO CREATE A COHESIVE, ADAPTIVE \rightarrow SECURITY FABRIC THAT GUARDS AGAINST BOTH HISTORICAL AND EMERGING THREATS.



for empowering businesses to anticipate and prepare for the continuously evolving future. Designed with interconnected and personalised features, the platform caters to users across all levels of operation - be it strategic, operational, or tactical - Reducing complexity and providing support through automated L1 and L2 tasks, effectively minimising resource expenditure attributed to human errors and concurrently enhancing the precision and performance of threat detection.

By automating routine processes such as patch management, vulnerability assessments, and incident response, organisations can alleviate the burden on their security teams and ensure that critical actions are taken promptly and consistently. This not only boosts efficiency but also minimises the risk of human error. Now, I'd be careless not to emphasise the importance of employee training and awareness. As the hybrid environment introduces new tools and procedures, it's imperative that everyone - from IT personnel to end-users — understands their role in maintaining security. Regular training sessions and awareness programs can go a long way in mitigating risks arising from human factors.

In terms of vendor partnerships,



organisations should opt for security solutions that seamlessly integrate with their hybrid architecture. This reduces the friction of managing multiple tools and platforms and enables streamlined security operations. Lastly, it's all about embracing a risk-based approach. Not all assets are equal, and not all threats pose the same level of danger. By conducting thorough risk assessments, organisations can prioritise their efforts on protecting the most critical assets. This way, they can allocate their resources more efficiently and effectively. It's about finding the right equilibrium between innovation and protection, and that's where the true strength of a hybrid security approach lies.

What are the potential cost implications of implementing a hybrid security approach? Is the investment justified by the level of protection it offers?

The financial implications of embracing a hybrid security approach can be deconstructed into several fundamental components. The initial capital outlay entails procuring and setting up a combination of hardware, software, and services tailored for both on-premises and cloud infrastructures. Though this initial expense might appear substantial,

it lays the foundation for a robust security stance. The subsequent consolidation and deployment of various security utilities might demand extra resources and time. However, the strengthening of security oversight could ultimately yield financial savings. Nevertheless, effectively managing a hybrid model necessitates a proficient team well-versed in both on-premises and cloud security methodologies, potentially resulting in training costs or augmented salaries. Nevertheless, this investment enhances the team's skills and readiness. Added to this, ongoing operational expenditures, encompassing licensing, upkeep, enhancements, and monitoring, can be efficiently controlled over time. Examining the justification of this investment in relation to protection level, a hybrid security approach offers numerous advantages that can be seen as returns on investment.

The fusion of on-premises and cloud-based solutions creates a robust defense mechanism covering a wider array of attack vectors. This heightened protection becomes indispensable as the cybersecurity landscape evolves and threats grow more sophisticated. The agility and flexibility intrinsic to a hybrid model empower businesses to swiftly adapt to changing security needs, enabling effective responses to emerging threats and compliance with evolving regulations. Moreover, the investment becomes particularly worthwhile when considering potential costs stemming from data breaches, downtime, and reputational harm. By minimising these risks, a hybrid approach mitigates financial losses and the expenses linked to recovery.

The hybrid strategy's role in facilitating regulatory compliance is another factor contributing to its justification. Many industries face stringent regulatory demands, and a hybrid model can aid in meeting these standards, thus avoiding substantial fines and legal consequences. Furthermore, the layered protection inherent to the hybrid approach bolsters business continuity, curbing the financial impact of cyber disruptions. Ultimately, in today's digital age, the guestion is not whether you can afford to implement a hybrid security approach, but rather, can you afford not to? The peace of mind and proactive protection it offers align with responsible business practices and the safeguarding of your organisation's digital future. It's an investment in resilience, and just like any sound investment, it requires careful consideration but has the potential for substantial returns in terms of mitigating risks and protecting your business in the long run.

Are there any regulatory or compliance considerations that organisations should be aware of when adopting a hybrid security strategy? How can they navigate these requirements effectively?

In today's intricate regulatory landscape, businesses are often subject to various industry-specific standards and regional data protection laws. Take, for instance, GDPR in Europe or HIPAA in the healthcare sector. When crafting a hybrid security strategy, organisations must ensure that their approach aligns with these regulations across all operational fronts – both on-premises and in the cloud.

First and foremost, a comprehensive assessment of the organization's regulatory requirements is essential. Identifying the specific laws and standards that apply to your industry and geographical reach will lay the foundation for your hybrid security approach. This assessment needs to extend across data handling, storage, and transmission practices, as well as access controls and breach notification procedures. Once the regulatory landscape is understood, the next step is to tailor the hybrid security strategy to encompass these considerations. This involves a fine balance between on-premises infrastructure and cloud services. Encryption and access controls become paramount to safeguard sensitive data. Additionally, robust monitoring and auditing mechanisms need to be in place to ensure compliance is maintained over time.

Collaboration between IT, legal, and compliance teams is key here. Regular communication ensures that all parties are on the same page and can work together to integrate regulatory requirements seamlessly into the hybrid security strategy. Moreover, staying up-to-date with evolving regulations is critical; these frameworks tend to change, and your hybrid strategy should be flexible enough to adapt. Leveraging industry best practices and frameworks, such as NIST Cybersecurity Framework or ISO 27001, can provide a solid foundation for building a compliant hybrid security approach. These standards offer guidelines that resonate with a wide range of regulatory requirements, making compliance more manageable.

Finally, the significance of substantial emplovee training must not be underestimated. The efficacy of any security strategy, whether hybrid or not, greatly hinges on the awareness and collaboration of the staff. Routine training workshops can furnish employees with the expertise needed to manage sensitive data judiciously and identify potential compliance challenges. In essence, while adopting a hybrid security strategy is a forward-looking move, organizations must never lose sight of their regulatory responsibilities. A well-thought-out approach that combines technology, collaboration, and ongoing education will ensure that the benefits of hybrid security are reaped without sacrificing compliance. At Bahwan CyberTek we believe, in the realm of cybersecurity, a proactive and holistic strategy is the true path to success.

What are the arguments against adopting a hybrid security approach? Are there scenarios where a fully traditional or fully modern approach might still be preferable?

In breaking down the concept of a hybrid security approach, this approach combines elements of both traditional and modern security strategies to create a comprehensive defense posture. Traditional methods usually involve well-established practices like firewalls, intrusion detection systems, and network segmentation. On the other hand, modern approaches leverage cutting-edge technologies such as AIdriven threat analytics, behavior-based detection, and cloud-native security tools. One argument against adopting a hybrid approach is the potential complexity it introduces. Managing a combination of older legacy systems alongside the latest tech can indeed be challenging. It might require specialised skill sets and

additional training for the security team, which can strain resources.

Moreover, the integration of diverse security solutions could lead to compatibility issues or gaps in coverage. It's like combining different puzzle pieces - sometimes they fit perfectly. but other times, you might end up with a few gaps that adversaries could exploit. Now, let's talk about scenarios where a fully traditional or fully modern approach might still hold value. In industries where compliance regulations dictate specific security measures, a fully traditional approach might be preferred. Industries like healthcare or finance often have stringent requirements that mandate proven, time-tested security practices.

On the flip side, industries that are heavily reliant on the agility and scalability of the cloud might lean more toward a fully modern approach. Cloudnative security tools can seamlessly adapt to dynamic environments and provide real-time threat insights that are crucial in today's rapidly evolving threat landscape. Ultimately, the decision on which approach to take boils down to a business's unique circumstances. Factors like budget, risk appetite, existing infrastructure, and the nature of the data being protected all play a role. It's a balancing act – finding the sweet spot that maximises security effectiveness while minimizing operational complexity.

At Bahwan CyberTek, our approach is always tailored to the specific needs of our clients. We aim to strike the right balance between legacy and innovation, understanding that each organisation's security journey is unique. The goal is to create a cohesive, adaptive security fabric that guards against both historical and emerging threats. In the grand scheme, the hybrid security approach is a testament to the ever-evolving nature of cybersecurity. It showcases the industry's willingness to learn from the past while embracing the future. As businesses continue to grapple with this decision, what remains constant is the imperative to stay vigilant, adapt, and always stay one step ahead of the adversaries. 🚺



O

17

Secure Your Digital Future Simple. Secure. Resilient.

Secure Your Enterprise IT Footprint For A Safer Digital Journey

> www.raqmiyat.com UAE | KSA | INDIA

INDICATOR OF ATTACK – WHAT COMES BEFORE A GOOD OLD INDICATOR?

EMAD HAFFAR, HEAD OF TECHNICAL EXPERTS FOR THE META REGION AT KASPERSKY & **DAMIR SHAYKHELISLAMOV**, ADVANCED THREAT PROTECTION SOLUTIONS MANAGER AT KASPERSKY

yberthreat detection has always been a trade-off between speed, accuracy, threat coverage, and the amount of information required to verify the security verdict.

The indicators of compromise (IoC) is one of the core aspects of cyber threat intelligence. Observable artifacts pointing to the presence of specific adversarial activities in the network infrastructure is what best describes IoC.

The simplicity of the concept itself and a variety of precise indicators (atomic or computed, network or host-based) presented as IP addresses, DNS names, JA3 TLS fingerprints, registry entries, or cryptographic hashes, along with the presence of numerous cyberthreat intelligence tools, open-source feeds, and exchange standards (STIX, Yara, OpenIOC) make them easily distributed, and digested by any automated technology (EDR/XDR, SIEM, NGFW, etc.).

However, despite being the most shared type of threat information, the operational limit of main IoC types (especially in combating complex threats) can be characterised by the attacker's low to moderate ease to evade defenders' detection capability. This is done by recompiling the code, modifying binary timestamps, changing URLs, etc. that usually results in IoC's short lifespan and high false positive rate.

From the attacker's perspective, a



good example of how to evade the IoCbased detection is by taking advantage of Domain Generation Algorithms used to generate pseudo-random domain names. These names are often used to establish more robust communications with the attacker's command and control (C2) servers. From the defenders' standpoint, this fact means blocking domains is an endless task, let alone being close to impossible to timely and effectively track.

Such a fundamental weakness of using low-level indicators was illustrated by the concept of the "Pyramid of Pain" presented by David J. Bianco almost ten years ago.

DGA-GENERATED NAME	VIRUSTOTAL URL DETECTION		
amdkwqwmsqouinswical.com	0/93		
ojeaoptwsysdgnrqdgci.com	0/93		
hnkbblscimtqdphbejua.com	0/93		
knwwmcelhsddclqecrte.com	0/93		
fqnvulpnfolpblclrmro.com	1/93		
noldclerowvakbkypokh.com	10/94		

The static nature of IoC-based detection and the post-breach view of the incident deprive the security analysts of the ability to examine what is happening behind the scenes when the attack is in progress. The widespread "fileless" persistence mechanisms (PowerShell, WMI, etc.) utilised by modern evasive malware, also lead to more meaningless forensic artifacts and observables, which make simple IoCs of little help.

Hunting down suspicious behaviour

As every activity on the enterprise infrastructure leaves its mark – and malicious cyber operations are not an exception – automating the process of spotting how attackers are switching between a variety of offensive tactics, techniques, and procedures (TTP) and raising corresponding red flags is a key step to keep up with a modern threat landscape.

The call for a new (proactive and more dynamic as opposed to traditional) detection approach was heard by the security industry. Today, the concept of threat indicators has dramatically evolved, making them more concerned with capturing behavioural characteristics and patterns of attack than solid and static artifacts.

These behaviour-based indicators, representing the attacker's modus

operandi, received the term Indicators of Attack (IoA); they enabled enhanced visibility of malicious techniques used during various phases of the attack cycle – from discovery to data exfiltration. For instance, the evidence of grabbing NTLM hashes by dumping the lsass.exe process followed by the subsequent execution of PowerShell script (with a hash value as a launch parameter) can be indicative of the pass-the-hash technique used to bypass normal access controls and move laterally through the infrastructure.

Looking at the screenshot above, alerts that are raised based on IoA

detections signifying bad or suspicious symptoms will be extremely helpful to security officers. When dealing with some devastating human-operated ransomware attacks, the ability to spot the signs of compromise long before the encryption process starts could be invaluable to timely cure the systems affected.

Less fragile from a defender's standpoint and hardest to dodge by attackers, IoA-based detection logic incorporated into threat protection technology stack helps to enrich the overall context of the threat actor's ultimate intent. It also ensures coverage

> TODAY, THE CONCEPT OF THREAT INDICATORS HAS DRAMATICALLY EVOLVED, MAKING THEM MORE CONCERNED WITH CAPTURING BEHAVIOURAL CHARACTERISTICS AND PATTERNS OF ATTACK.

VIP	Created	Detected	Details
-	2022-06-17 16:41:13	obfuscated_powershell_ amsi	Hosts: 1
_	2022-06-17 16:41:13	suspicious_powershell_c mdline_general_obfuscat ion_amsi	Hosts: 1
-	2022-06-17 16:41:13	query_registry_for_store d_credentials_amsi	Hosts: 1
-	2022-06-17 16:41:13	pass_the_hash_attack_in put	Hosts: 1
-	2022-06-17 16:41:13	pass_the_hash_attack_a msi	Hosts: 1

Lateral movement: series of IoA alerts triggered by Invoke-TheHash scripts (EDR solution)

EXCLUSIVE / KASPERSKY

of detection for wider clusters of malicious objects, and defines rapid remediation efforts.

The concept has found its special recognition and become the key driving force in Endpoint Detection and Response (EDR), emerging Extended Detection and Response (XDR), SIEM tools, and security service offerings such as Managed Detection and Response (MDR).

IoA's are highly instrumental when hunting for the heavily leveraged "living off the land" techniques. In their attempts to evade detection and 'blend in', attackers exploit trusted, legitimate, and dual-use OS tools (scripting engines, binary utilities, etc.) to blind monitoring solutions and get off the security radars.

No matter the OS, the range of actions available at the post-exploitation phase is enormously wide – whether it is the creation of new user accounts, deleting disk shadow copies, or attempts to disable existing security mechanisms – a carefully created IoA rules can alert for any suspicious sequence of events covering a wide range of scenarios.

Due to the probabilistic nature of the detection process, not all IoA-triggered



events shall be treated with equal importance. Using netsh.exe utility to add some local firewall rule exception or using schtasks task scheduler can be considered as a weaker signal in comparison with attempts to execute highly obfuscated Powershell scripts (MITRE T1027) or patterns known to dumping credentials from Isass process memory (MITRE T1003). Therefore, assigning an indicator's severity level based on expert-opinion (by the rule vendor or the user) is essential for an adequate alert triage process and to achieve optimum resource allocation tactics.

Provided that sufficient coverage by regularly updated IoA ruleset exists, the chances of raising attention of the defenders as a threat actor progresses and attempts to maintain their persistent within the infrastructure are quite high.

What are the requirements to implement effective behavioural detection?

Data acquisition and processing

Firstly, detecting attack patterns using IoA requires acquiring and storing raw telemetry/log data from all relevant sources. Filtering and aligning event data to a common format (normalisation) is required – depending on the used tools, each vendor specifies the optimal amount of data and normalisation standards. As part of the process, the IoA engine queries the current event repository and extracts actionable intelligence in the form of tactics, techniques, and procedures.

Multi-source signals

When addressing some targeted and sophisticated campaigns, no event could be strong enough to diagnose the threat scope, thus correlation of multiple signals (sometimes 'weak' to confidently raise a single incident) is required for further investigation. Using endpoint, network, or cloud sources for IoA rule



Indicators of Attack	Indicators of Compromise		
 Proactive - search for warning signs of attack (focus on behavioral markers) Ability to detect unknown threats i.e., when attacker's activity is masked as legitimate 	 Reactive – signals that attack has occurred Precise detection mechanism – artifacts can be easily uploaded into wide list of security tools (i.e., prevention-focused) Less resource intensive ("simple matching") 		
 Expertise is required- especially for creating new rules and dealing with false positives Requires aggregation of telemetry 	 Known threats can be addressed Relatively fast expiration Requires regular IoC database updates 		

engineering is the key to recognizing hidden, and temporal dependencies between seemingly unrelated activities.

Retention and retrospective analysis

The duration of cyber-offense operations could be lengthy, so long-term retention of historical telemetry data () can be a good practice to be able to look backward for detection of previously unseen threat activities by re-applying a regularly updated set of IoA rules.

Data exchange

The intelligence lifecycle is unthinkable without the phase of distribution of actionable threat-related data across other interest groups (in our case, machine-readable behavioural rules). Traditionally, when describing IoA rules, security vendors tend to define their specification language and sharing schemes – the lack of easily adoptable and commonly accepted standard presents a challenge for the industry, so further unification efforts (e.g., SIGMA language) seem promising.

Tailoring behaviour indicators to current infrastructure

Each organisation is unique and local context matters when talking about targeted attacks. Although an evergrowing industry-recognised knowledge base of adversarial tactics and techniques (such as MITRE ATT&CK) is incorporated into a great number of out-of-thebox vendor rules, the ability to extract additional detection opportunities from practical observations, and produce its own set of indicators is a great way to perform hunting activities more effectively.

Whether it would be the uploads of code fragments to the Github repository, execution of some binaries not used in practice by the DevOps team, policy violations, or tracking some previously unseen Command & Control beaconing patterns – using IoA, the analyst can establish detection engineering process

10.2544	New	IOA.	access_to_mailcious_horts_from_nontprovisers_network_activity_by_process_with_exact_detect	Device: User	whilesole which to share a strategy of the str
0.245	New	OA.	suprovuluefullunage_downloading_or_remote_interaction	Dever	unitariola unitarioleficationical
945.0 B	New	64	Net_ie_adoblet_netwol_lie_system_processes, procidurg_sdurp_hass	Device: Unit	whitpold www.phoen.idennueue
E 2,2541	New	i0A	mmilalz, comments, palteris, windows, credentals, durging, tools, behaviour, detect, usg-close, cer-	User Device.	WW00PR064-Administration with Digwood Administration
0.540	New	icia.	windows, credentiate_durrying, tools, behaviour, defact, suspicious, centuiti, usage_decoding	Device. Unit	windbps44 windsPR0540Administrati
10.25M	New	64	suprovul, cefull, usge, downloeding, or, remote_interaction, suspicious, certuil_usage, decoding	UNER Device	VINCEPTOS4 Administra VINCEPTOS4 Administra
0.25N	New	OK.	network_activity_by_process_with_exact_detect_access_tex_malicious_hosts_borm_nonbrowsers_scape.	User Devce	ismos/HolesAdhimated web3prol4
E 10250	New	10A	proclump_stump_hass_lies_in_autostart_numed_like_system_processes	Deves: Uwe	while set and
12.25M	New	ios.	mmist/_communit_patiens, suspiciour_central_usage_downstading_or_minist_meraction_cease.	Device: Unit	whitepole whiteProferAdministra
0.2525	New	104	windows, credentials, duriging, tools, behaviour, detect	Devis: Unit	weblpold weblphold Administra
0.054	New	iQK.	swaruove_certuil_usage_decoding	Devia. Unit	windbardek windbinkolenkammana
825.0 =	New	-	suspicious, certuill_ussige_écomice.ding_or_remons_interaction	Device	whitipist4 whitipist4

and automate testing of detection hypotheses. The latter requires specific expertise in place for proper tuning.

The ability to set the exceptions and temporarily disable certain behavioural indicators from the processing might also be a reasonable step in efforts to minimise the overall noise level, e.g., whitelisting of activities associated with specific administration tools.

We should remember there is always room for further automation – whether it will be adding more log sources, creating a global and shareable repository of indicators, or applying machine learning techniques to detections to enhance an alert confidence scoring.

Summary

Behavioural correlation of events from multiple sources helps to act faster, get more attack context and start looking for previously unseen activities.

None of the detection technologies and approaches shall be considered a silver bullet. Being the most trivial threat intelligence unit, the significance of using classic indicators of compromise should not be undervalued – atomic indicators are precise, easy to apply, share, and multiple machine-readable formats are available. Not so many organisations use even this form of threat data efficiently.

The following comparison matrix highlighting key features of detection approaches, demonstrates that taking the best of both methods is required to better understand an attacker's tradecraft.



RE-EXAMINING THE ROLE OF THE CISO

EZZELDIN HUSSEIN, REGIONAL DIRECTOR, SALES ENGINEERING AT SENTINELONE

igital transformation is changing the business models of industries and enterprises. It is also changing the roles of

employees, team leaders, and C-suite executives. Amongst them the role of the Chief Information Security Officer (CISO) has also come under pressure to change and adapt to the growing pressures of the macro environment, the position of the digital enterprise, and the future capabilities of the role of CISO.

At one time the role of the CISO focused on championing the implementation of digital security strategies. Previously, CISOs focused on technical aspects of security, such as implementing and managing security technologies. However, the sophistication of cyberattacks has created a need for a much broader approach to cybersecurity. In today's landscape, successful CISOs must now deliver the mantle of risk manager and communicator. Any CISO that can identify the risks that digital enterprises face as it transforms, and shares them effectively, in an actionable way inside the enterprise, is better suited to grow.

CISOs are not only instrumental in implementing and managing the enterprise's cybersecurity strategy but


also to ensure that employees are aware of cybersecurity best practices and are trained to identify potential threats. They also act as a link between employees and senior leadership and stakeholders, and CISOs are responsible for communicating effectively with both groups about the enterprise's cybersecurity posture.

The capability of the CISO to deliver this role, namely understanding the risks in the digital landscape and communicating them internally, directly impacts the short and long-term security profile of the enterprise.

Other than regular security assessments and implementing the latest security measures, the role of the CISO now involves much more collaboration and coordination with other departments and partners. Cyber threats cross organisational boundaries, and effective cybersecurity requires a coordinated response from all parties.

Today's role of the CISO is a balancing act across five different independent areas. The capability of the CISO to act and deliver needs to be balanced across all these five independent areas:

1. Risk Management

Through regular risk assessments, CISOs can identify and assess potential risks to the enterprise's assets, such as data, systems, and networks. A large part of the risk management strategy will cover how the enterprise will implement controls to prevent or mitigate identified risks.

2. Strategic Communication

Successful CISOs exhibit communication skills and prioritise sharing the enterprise's cyber strategy to build trust. CISOs are also masters of knowing their audience and are able to determine who needs to be informed about the enterprise's cyber risk management strategy.

3. Leadership in Managing Resources

Technical and IT teams will look to their CISO to implement cost-effective controls. Understanding the cost and benefits of different controls and having the ability to choose those that provide the most value for the enterprise is vital.

4. Continuous Learning

It is important to offer a variety of training options such as in-person training, online courses, and webinars, to make it easier for employees to participate, and use real-world examples and case studies to illustrate the importance of cybersecurity and the potential consequences of security breaches.

5. Security Expertise

Since the cybersecurity landscape is evolving, CISOs need the ability to adapt to new threats and technologies. Being up-to-date on the latest trends and developments in the field allows a CISO to ensure their enterprise's strategy is in tune with the times. Having sound technical acumen also allows someone in the role to take calculated risks.

Enterprises require multi-layered security strategies to combat advanced cyber threats. Bringing all the pieces together requires a CISO who understands what the business needs and translates that into security policies and processes. Critical success factors for CISOs lie in their ability to coordinate traditional implementation with modern security analytics and continuous improvement.

Today's successful CISOs are highly skilled and knowledgeable leaders who possess deep understanding of technology, as well as business acumen and strong communication and leadership abilities. They are strategic thinkers able to anticipate risks and adaptable to the changing cybersecurity landscape. Most importantly, they must be ethical and trustworthy leaders who are committed to upholding the values of the enterprise business.

STAYING SUSTAINABLE

ANITA JOSEPH CAUGHT UP WITH **TERTIUS WOLFAARDT,** ARCHITECTURE & ENGINEERING MANAGER AT AXIS COMMUNICATIONS, TO FIND OUT MORE ABOUT SUSTAINABLE TECH AND HOW AXIS IS INCORPORATING SUSTAINABILITY INTO ITS PRODUCTS AND SOLUTIONS.

ow important is sustainable tech? Organisations across all industries are increasingly adopting sustainable practices. This is being largely driven by consumers, from retail customers through to users of public services such as transport or healthcare. The push to greater sustainability is also being made by investors and wider stakeholders, including politicians, campaigners and even celebrities.

Environmental considerations are vital, but today, sustainability involves far more, not least social and economic requirements. Globally recognised sustainable development goals (SDGs) are presented in the UN Global Compact, and there's also a practical need for organisations to take action. Just as greenwashing can negatively impact reputation, consumers are also looking for sustainable practices that span all organisational operations.

While network cameras are just one part of a business's operational technology, it's important for an organisation to partner with a technology provider they can trust to uphold values in sustainability. An organisation's credentials can be undermined through a partnership that isn't sustainable. This means that technology manufacturers need to demonstrate ethical behavior throughout all their relationships, as well as developing products that minimise environmental impact.

Working with the right camera provider can help an organisation, such as a business or city authority, improve the sustainability of the service they provide. To achieve this, it's key to work with a supplier that can not only provide the right technology, but who also has their own strong sustainability credentials.

How is Axis integrating sustainability into its solutions and services?

Acting sustainably means creating long-term stakeholder value through the implementation of a business strategy that focuses on people, planet, and prosperity. At Axis, we know that sound business practices are crucial for the future of a company, and that caring for people and the environment makes good business sense. We act responsibly, and have a sustainable approach across the entire value chain. Axis is in it for the long run. Our business model is based on close partnerships based on mutual trust. We set high ethical standards, and handle all relationships transparently, and with care. We also strive to contribute to the many local communities where we are present. We are a leader in our industry and have a long-term approach to everything we do. We want to contribute to a smarter, safer world, and be a role model that inspires positive changes in society. We strive to influence and raise industry standards, and work closely with decision-makers and stakeholders to this end.

How is this new approach helping the company align with UAE's sustainability goals?

The UAE primarily focuses on the SDGs that enable access to clean energy, sufficient food at reasonable prices, guality education and healthcare, alongside creating sustainable economic growth, healthy environmental systems, and increased resource efficiency. Axis signed the UN Global Compact 2007, and our strategies and operations are aligned with these universal principles on human rights, labor, environment, and anti-corruption. The UN goals and the UAE goals closely related in their objectives. We also support the 17 Global Sustainable Development Goals (SDGs) of the UN 2030 Agenda, which act as a blueprint for peace and prosperity for people and the planet.



What are the key measures / metrics that Axis has been able to achieve with its sustainability approach?

Axis meets the demands in the EU's directive on the restriction of certain hazardous substances in electrical and electronic equipment: equipment (the RoHS Directive), and the requirements in the EU's directive on the collection and recycling of electrical and electronic equipment (WEEE). We also meet the requirements in the EU Waste Framework Directive and in the EU's regulation on Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), which aims to control/eliminate dangerous substances. Axis products contain a variety of materials, such as aluminum. zinc. steel. stainless steel. polycarbonate/ acrylonitrile butadiene styrene, polycarbonate, polyamide, polymethylmethacrylate, polyurethane, silicone, thermoplastic elastomer, and rubber. We have a list of banned and restricted substances, including both substances that are already regulated by law, and substances that aren't restricted yet, but will likely be so in future. The list includes plasticisers, as well as brominated and chlorinated flame retardants (BFRs and CFRs). It's very important to us to not just wait for new legislation, but rather be one step ahead. This proactivity is a competitive advantage, ensuring we are ready for upcoming legal regulations, creating a more robust business, and enabling us to offer customers products that are free from hazardous substances. 65 percent of all cameras launched in 2022 were BFR/CFR-free. In total, approximately 90 percent of Axis network cameras and encoders launched in 2022 were PVC-free. We monitor our progress yearly. Greensoft is a software solution and part of our



HPDP-process that makes it possible for us to more systematically collect and validate data relating to product content. This means we get a better overview of the content in various materials, an important step process of increasing the use of materials that have a lower environmental impact. BFR/CFR and PVC The development of cameras that are free of hazardous BFR (brominated flame retardants) and CFR (chlorinated flame retardants), without compromising fire safety, was a key milestone on our goal to minimise and, eventually, avoid the use of hazardous substances. We have ambitious targets to reduce both BFR and CFR. The goal is that 100 percent of all indoor cameras launched in 2022, and all cameras launched in 2024, will be BFR/ CFR-free, and all Axis designed products launched in 2025 should be PVC/BFR/ CFRfree. PVC can emit toxic substances, and is harmful to both human health and the environment. It is also difficult to recycle. We are striving to phase out PVC from our products and are well on track. The goal is that 100 percent of all launched Axis products should be

PVC-free by 2025. In total, approximately 90 percent of Axis network cameras and encoders launched in 2022 are PVC-free.

GOALS | 2022: 100% BFR/CFR-free network cameras launched 2024. 2022 | 65% achieved 100% BFR/CFR-free PCBAs in cameras launched 2022. 2022 | 75% achieved 100% BFR/CFR-free indoor cameras launched 2022. 2022 | 68% achieved

What solutions are specially created / curated with sustainable tech?

Video surveillance has played a central role in the liveability of cities for many years of course, particularly in keeping citizens safe and secure. The increasing sophistication of video surveillance technology – particularly related to video analytics and the ability to link data from sensors of multiple types, including video cameras – means that it can support a number of the challenges facing cities and specifically the SDGs smart cities are looking to accomplish.

Three of the fundamental areas that cities are focused on, and which directly relate to a number of SDGs are the environment, mobility and public safety. And far from being independent of each other, these factors are very much interlinked. Again, this reinforces the critical need to break down silos and enable data sharing across the city and, as stated in SDG 17, partnerships are the main enabler of success in sustainability targets. **1**

ACTING SUSTAINABLY MEANS CREATING LONG-TERM STAKEHOLDER VALUE THROUGH THE IMPLEMENTATION OF A BUSINESS STRATEGY THAT FOCUSES ON PEOPLE, PLANET, AND PROSPERITY.

Allied Telesis



Next Generation Industrial Switches

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

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

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



Tel: +971 4 3522 433

AI IS HERE: HOW SHOULD CISOS RESPOND? GAIL COURY, SVP AND CISO, F5



ith Artificial Intelligence (AI) use growing, Chief Information Security Officers (CISOs) play

a critical role in its implementation and adoption. They need to prepare for the risks associated with AI content creation as well as AI-assisted security threats from attackers. By following some key best practices, we'll be better prepared to safely welcome our new robot overlords into the enterprise!

Al is growing fast!

The popularity of ChatGPT has sparked massive interest in the potential of generative AI and many businesses are deploying it across the enterprise. AI technology is now in the wild—and it's moving faster than any other technology I've seen. There are several compelling use cases for generative AI in the enterprise:

- **Content Creation:** Tools such as ChatGPT can assist content creators in generating ideas, outlines, and drafts—potentially saving individuals and teams significant time and effort.
- Learning and Education: Properly trained AI tools can be used to quickly understand new and complex subjects by summarizing large amounts of

information, answering questions, and explaining complicated concepts in simple language.

- Coding Support: Tools like GitHub Copilot and OpenAl's API Service can help devs write code more efficiently and identify errors for queries.
- **Product and Operations Support:** Tools can be used to more efficiently prepare common reports and notices, such as bug resolutions.

Issues and challenges

However, there are challenges to overcome, such as whether using AI at all will run afoul of laws and regulations in international markets.

Earlier this year OpenAI temporarily blocked the use of ChatGPT in Italy after the Italian Data Protection Authority accused it of unlawfully collecting user data. Meanwhile, German regulators are looking at whether ChatGPT adheres to the European General Data Protection Regulation (GDPR). In May, the European Parliament took a step closer to issuing the first rules on use of Artificial Intelligence.

Another challenge are the issues around data collection and the accidental disclosure of personal or proprietary information. Companies need to secure their confidential information against and ensure they aren't plagiarising from other companies and individuals who are using the same tools they are. We've already seen reports of intellectual property being entered into public generative AI systems, which could impact a company's ability to defend its patents. One AI-powered transcription and note-taking service makes copies of any materials that are presented in Zoom calls that it monitors.

The third major challenge is that Alpowered cyberattack software could try many possible approaches, learn from how we respond to each, and quickly adjust its tactics to devise an optimal strategy—all at a speed much faster than any human attacker. We have seen new sophisticated phishing attacks that are utilising AI, including impersonating individuals both in writing and in speech. For example, an AI tool called PassGAN, short for Password Generative Adversarial Network, has been found to crack passwords faster and more efficiently than traditional methods.

CISOs and AI

As CISOs, we help leaders create an organisational strategy that provides guidelines for use and takes into account legal, ethical, and operational considerations.

When used responsibly and with proper governance frameworks in place, generative AI can provide businesses with advantages ranging from automated processes to optimisation solutions.

Creating a comprehensive AI strategy

With new technologies such as generative AI, come opportunities. But they also come with risks. A comprehensive AI strategy ensures privacy, security, and compliance, and needs to consider:

- The use cases where AI can provide the most benefit.
- The necessary resources to implement AI successfully.
- A governance framework to manage the safety of customer data and ensure compliance with regulations and copyright laws in every country where you do business.
- Evaluating the impact of Al implementation on employees and customers.

A company's AI strategy should cover how changes brought about by AI automation will affect employees and customers. Employee training initiatives can help ensure that everyone understands how these new technologies

A COMPANY'S AI STRATEGY SHOULD ALSO COVER \rightarrow HOW CHANGES BROUGHT ABOUT BY AI AUTOMATION WILL AFFECT EMPLOYEES AND CUSTOMERS.

are changing day-to-day processes and how threat actors may already be using them to further increase the efficacy of their social engineering attacks. Customer experience teams should assess how changes resulting from AI implementation might impact customer service delivery so that they can adjust accordingly.

Al and security

Al tools need to be designed with adversarial robustness in mind. We currently see this happening in the lab to improve training, but doing this in the 'real' world, against an unknown enemy, must be top-of-mind—especially in military and critical infrastructure scenarios.

With attackers looking closely at Al, your organisation needs to plan and prepare their defense right now. Here are a few practices to consider:

- Ensure you analyse your software code for bugs, malware, and behavioral anomalies. Signature 'scans' only look for what is known, and these new attacks will leverage unknown techniques and tools.
- When monitoring your logs, use AI to fight AI. Machine Learning security log analysis is a great way to search for patterns and anomalies. It can incorporate endless variables to search for and produce predictive intelligence, which in turn provides predictive actions.
- Update your cybersecurity training to reflect new threats such as Al-powered phishing, and your cybersecurity policies to counter the new Al password cracking tools.
- Continue to monitor new uses of AI, including generative AI, to stay ahead of emerging risks.

These steps are critical to building trust with your employees, partners, and customers about whether you're properly safeguarding their data.

To stay competitive, it's essential for organisations to adopt AI technology while safeguarding against potential risks. By taking these steps now, companies can ensure they're able to reap the full benefits of AI while minimising exposure.

SECURING INDUSTRIAL SUPPLY CHAINS

WILLIAM HUTCHISON, CEO AT SIMSPACE, TELLS ANITA JOSEPH HOW SECURITY TEAMS RESPONSIBLE FOR PROTECTING DISTRIBUTION COMPANIES NEED TO BRING A MILITARY MINDSET TO THEIR PREPARATIONS AND TRAIN TO FAILURE LIKE AN ARMY OR NAVY.



hat are the latest challenges for companies in the area of cybersecurity both in terms of what the "bad actors" are doing, as well as from a regulatory/standards perspective (CMMC 2.0) to prevent hacking to supply chain partners? Industrial supply chains are complex and interdependent. Third parties are often experts in their business, but not necessarily cybersecurity. It can only take one business failing in a supply chain for all of their partners to be similarly breached.

The 2022 Verizon Data Breach Investigations Report states that 62 percent of cyber incidents caused by system intrusion involved compromised third-party partners. According to Gartner, cyberattacks related to third parties are increasing. However, only 23 percent of security and risk leaders monitor third parties in real-time for cybersecurity exposure. Third-Party Risk Management (TPRM) is the process of analysing the risks associated with your supply chain and working to minimise those risks. This type of analysis will reveal that companies are facing a litany of threats, both to themselves and via their partners.

Threats arrive in the shape of insider threats, social engineering, DDoS attacks, ransomware, advanced persistent threats, software vulnerabilities, data breaches, compliance, and cross-border data transfers.

Distribution companies also need to comply with the latest regulation which seeks to standardise cybersecurity preparedness. For example, the Cybersecurity Maturity Model Certification (CMMC 2.0) is a framework designed by the Department of Defense (DoD) to implement cybersecurity best practices for contractors. This involves encrypting data in transit and at rest so it can't be breached, implementing access control measures, and establishing incident response procedures. There are a range of other certifications supply chain businesses may need to comply with such as ISO 27001 STAR Level 2, an independent assessment of the security of a cloud service provider and NIST SP 800-161, a set of guidelines for identifying, assessing, and mitigating supply chain systems, components, and services risks.

The best way to prepare a business's people, processes and technology to be ready under emergency conditions is to mimic attacks in a cyber range environment. Cyber ranges, simulated replicas of a company's networks and systems, also provide a good source of data to supply to regulators about the steps a company is taking to defend their systems. Cyber range events can involve multiple organisations to establish end-to-end security best practices and requirements.

What are the big trends and/or developments in cybersecurity defensive technologies for distribution companies today?

It's difficult to look past Russia's invasion of Ukraine as the most important trend in the cyber world. As well as attempting to disable Ukraine's systems, Russia is waging a hybrid war with the west, using cybercrime to damage businesses and steal sensitive information without directly entering into an explicit conflict. War has traditionally been fought on four

BUSINESSES SHOULD INCLUDE THEIR SUPPLY CHAIN PARTNERS IN THEIR SECURITY AUDITS, LIVE-FIRE EXERCISES, RISK ASSESSMENTS AND EMPLOYEE TRAINING.

fronts: land, sea, air and via economic sanctions. Cyber is now undoubtedly the fifth plane by which Russia and other state-actors like North Korea and Iran seek to cause damage.

Because they are for all intents and purposes at war, security teams responsible for protecting distribution companies need to bring a military mindset to their preparations and train to failure like an army or navy. Only by stress-testing their readiness with combat-like simulations can businesses and their stakeholders gain visibility into their strengths and vulnerabilities.

As criminals continue to hone their tactics, techniques and procedures, so security teams need to drive continuous improvements. Businesses should include their supply chain partners in their security audits, live-fire exercises, risk assessments and employee training. Gartner expects that by 2025, 60 percent of organisations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements.

How has your company responded to the changing environment to help distribution companies be safe from cyber-attacks? (talk about what is important and distinctive about your products/services in detail if you wish) The sophistication of cybercrime has rapidly made cybersecurity a primary focus for businesses in the distribution industry. In the last month, President Biden's national security strategy made the "resilience of critical infrastructure and the essential services it provides" one of the five pillars needed for a cyber-secure country. Where there wasn't a minimum standard for cybersecurity accountability before,

legislators and regulators are now making assurances. They are also proposing wide-ranging regulation such as the SEC's proposed legislation that would make it mandatory for publicly listed companies to declare cyber incidents within 4 working days. Gartner found that 60% of directors list compliance measures as their number 1 concern.

Rather than simply focusing on a company's servers or devices, organisations now recognise the importance of securing their entire IT infrastructure, including third-party applications and their operational technology (OT) systems.

Attacks initiated on large, wellresourced companies are now part of a war that requires private sector industries to better manage their security risks. SimSpace's Cyber Force Platform allows commercial sector organisations to use the same government-grade cyber ranges that have been tried and tested by nation states and intelligence agencies around the world.

Our cyber range technology originates in the MIT Lincoln Laboratory, and can emulate a company's entire network in a safe, simulated environment. The highfidelity nature of the range circumvents the possibility of damaging or corrupting real-world systems. Instead, it allows offensive and defensive teams to test and train their network with the same robust complexity, but without the adverse consequences of testing inproduction. This results in a 30% cost saving on security operations and a 40% improvement for cyber detection and remediation, increasing visibility for auditors, executives and insurers to get answers to the tough cybersecurity questions they are asking. 🚦

Q2 2023 CHARACTERISED BY PERSISTENT WAVES OF DDoS ATTACK CAMPAIGNS: CLOUDFLARE

loudflare, Inc., the security, performance, and reliability company helping to build a better Internet, has announced its 2023 Q2 DDoS report. This report includes insights and trends about the DDoS threat landscape — as observed across the global Cloudflare network.

The DDoS landscape: a look at global patterns

The second quarter of 2023 was characterised by thought-out, tailored and persistent waves of DDoS attack campaigns on various fronts, including:

- Multiple DDoS offensives orchestrated by pro-Russian hacktivist groups REvil, Killnet and Anonymous Sudan against Western interest websites.
- An increase in deliberately engineered and targeted DNS attacks alongside a 532% surge in DDoS attacks exploiting the Mitel vulnerability (CVE-2022-26143). Cloudflare contributed to disclosing this zero-day vulnerability last year.
- Attacks targeting Cryptocurrency companies increased by 600%, as a broader 15% increase in HTTP DDoS attacks was observed. Of these, there is an alarming escalation in attack sophistication.

Additionally, one of the largest attacks this quarter was an ACK flood DDoS attack which originated from a Miraivariant botnet comprising approximately 11K IP addresses. The attack targeted an American Internet Service Provider. It peaked at 1.4 terabit per seconds (Tbps) and was automatically detected and mitigated by Cloudflare's systems.

Despite general figures indicating an increase in overall attack durations, most of the attacks are short-lived and so was this one. This attack lasted only two minutes. However, more broadly, Cloudflare has seen that attacks exceeding 3 hours have increased by 103% QoQ.

Sophisticated HTTP DDoS attacks

An HTTP DDoS attack is a DDoS attack over the Hypertext Transfer Protocol (HTTP). It targets HTTP Internet properties such as websites and API gateways. Over the past quarter, HTTP DDoS attacks increased by 15% quarter-over-quarter (QoQ) despite a 35% decrease year-over-year (YoY). Additionally, there has been an alarming uptick in highly-randomized and sophisticated HTTP DDoS attacks over the past few months.

Protecting websites against sophisticated HTTP DDoS attacks requires intelligent protection that is automated and fast, that leverages threat intelligence, traffic profiling and Machine Learning/statistical analysis to differentiate between attack traffic and user traffic. Moreover, even increasing caching where applicable can help reduce the risk of attack traffic impacting your origin. Read more about DDoS protection best practices here.

DNS Laundering DDoS attacks

The Domain Name System, or DNS, serves as the phone book of the Internet. By disrupting DNS servers, attackers impact the machines' ability to connect to a website, and by doing so making websites unavailable to users.

Over the past quarter, the most common attack vector was DNS-based DDoS attacks — 32% of all DDoS attacks were over the DNS protocol. Amongst these, one of the more concerning attack types we've seen increasing is the DNS Laundering attack which can pose severe challenges to organisations that operate their own authoritative DNS servers.

The term "Laundering" in the DNS Laundering attack name refers to the analogy of money laundering, the devious process of making illegally-gained proceeds, often referred to as "dirty money," appear legal. Similarly, in the DDoS world, a DNS Laundering attack is the process of making bad, malicious traffic appear as good, legitimate traffic by laundering it via reputable recursive DNS resolvers. A large Asian financial institution and a North American DNS provider are amongst recent victims of such attacks.

Similar to the protection strategies outlined for HTTP applications, protecting DNS servers also requires a precise, fast, and automated approach. Leveraging a managed DNS service or a DNS reverse proxy such as Cloudflare's can help absorb and mitigate the attack traffic. For those more sophisticated DNS attacks, a more intelligent solution is required that leverages statistical analysis of historical data to be able to differentiate between legitimate queries and attack queries.

The rise of the Virtual Machine Botnets

The era of VM-based DDoS botnets has

arrived and with it hyper-volumetric DDoS attacks. These botnets are comprised of Virtual Machines (VMs, or Virtual Private Servers, VPS) rather than Internet of Things (IoT) devices which makes them so much more powerful, up to 5,000 times stronger. These botnets have executed one largest recorded DDoS attacks including the 71 million request per second DDoS attack. Multiple organisations including an industryleading gaming platform provider have already been targeted by this new generation of botnets.

Cloudflare has proactively collaborated with prominent cloud computing providers to combat these new botnets. Through the quick and dedicated actions of these providers, significant components of these botnets have been



neutralised. Since this intervention, Cloudflare has not observed any further hyper-volumetric attacks yet, a testament to the efficacy of the company's collaboration.

"Startblast": Exploiting Mitel vulnerabilities for DDoS attacks

In March 2022, we disclosed a zero-day vulnerability (CVE-2022-26143), named TP240PhoneHome, which was identified in the Mitel MiCollab business phone system, exposing the system to UDP amplification DDoS attacks.

Overall, in the past quarter, Cloudflare has seen additional emerging threats such as DDoS attacks abusing the TeamSpeak3 protocol. This attack vector increased by a staggering 403% this quarter. TeamSpeak, a proprietary voice-over-Internet Protocol (VoIP) that runs over UDP to help gamers talk with other gamers in real time. DDoS attacks that target TeamSpeak servers may be launched by rival groups in an attempt to disrupt their communication path during real-time multiplayer games and thus impact their team's performance.

DDoS hotspots: The origins of attacks

Overall, HTTP DDoS attacks increased by 15% QoQ despite a 35% decrease YoY. Additionally, network-layer DDoS attacks decreased this quarter by approximately 14%. In terms of total volume of attack traffic, the US was the largest source of HTTP DDoS attacks. Three out of every thousand requests we saw were part of HTTP DDoS attacks originating from the US. China came in second place and Germany in third place.

Industries under attack: examining DDoS attack targets

When examining HTTP DDoS attack activity in Q2, Cryptocurrency websites were targeted with the largest amount of HTTP DDoS attack traffic. Six out of every ten thousand HTTP requests towards Cryptocurrency websites behind Cloudflare were part of these attacks. This represents a 600% increase compared to



the previous quarter. After Crypto, Gaming and Gambling websites came in second place as their attack share increased by 19% QoQ. Marketing and Advertising websites not far behind in third place with little change in their share of attacks.

The Media & Newspaper industries were the most attacked in the Middle

East. The vast majority of attack traffic originated from Europe (74%).

Countries and regions under attack: examining DDoS attack targets

When examining the total volume of attack traffic, last quarter, Israel leaped to the front as the most attacked country. This quarter, attacks targeting Israeli websites decreased by 33% bringing it to the fourth place. The US takes the lead again as the most attacked country, followed by Canada and Singapore. If we normalise the data per country and region and divide the attack traffic by the total traffic, we get a different picture. Palestine jumps to the first place as the most attacked country. Almost 12% of all traffic to Palestinian websites were HTTP DDoS attacks.

Ransom DDoS attacks

Occasionally, DDoS attacks are carried out to extort ransom payments. Unlike Ransomware attacks, where victims typically fall prey to downloading a malicious file or clicking on a compromised email link which locks. deletes or leaks their files until a ransom is paid, Ransom DDoS attacks can be much simpler for threat actors to execute. Ransom DDoS attacks bypass the need for deceptive tactics such as luring victims into opening dubious emails or clicking on fraudulent links, and they don't necessitate a breach into the network or access to corporate resources.

Over the past quarter, reports of Ransom DDoS attacks decreased. One out of ten respondents reported being threatened or subject to Ransom DDoS attacks.

Commenting on the report, Bashar

$\begin{array}{l} \textbf{DESPITE GENERAL FIGURES INDICATING AN} \\ \rightarrow \textbf{INCREASE IN OVERALL ATTACK DURATIONS, MOST} \\ \textbf{OF THE ATTACKS ARE SHORT-LIVED.} \end{array}$

Bashaireh, Managing Director & Head of Sales - Middle East and Türkiye at Cloudflare, "In recent months, there's been an alarming escalation in the sophistication of DDoS attacks. And even the largest and most sophisticated attacks that we've seen may only last a few minutes or even seconds — which doesn't give a human sufficient time to respond."

"Security is not one single product or a click of a button, but rather a process involving multiple layers of defense to reduce the risk of impact. Cloudflare's automated DDoS defence systems consistently safeguard our clients from DDoS attacks, freeing them up to focus on their core business operations. These systems are complemented by the vast breadth of Cloudflare capabilities such as firewall, bot detection, API protection and even caching which can all contribute to reducing the risk of impact. The DDoS threat landscape is evolving and increasingly complex, demanding more than just quick fixes. Thankfully, with Cloudflare's multi-layered defenses and automatic DDoS protections, our clients are equipped to navigate these challenges confidently. Our mission is to help build a better Internet, and so we continue to stand guard, ensuring a safer and more reliable digital realm for all." 1



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

NEVER SAY DIE

OUR PERSONALITY OF THE MONTH (SECURITY) IS **JAVED ANSARI**, MARKETING MANAGER-MEA, EDGIO.



ell us about yourself-your career background, how long you've been in the Middle East and what your current responsibilities are.

After completing my MBA in marketing and B.Tech in Mechanical Engineering, I've had the immense pleasure of working in the marketing domain since 2008. I am passionate about my work. Over the years, I have been part of multi-national companies like Omron, Western Digital and Edgio (previously known as Limelight Networks). On the agency side, I have been part of team managing marketing communication campaigns for brands like Electrolux, Zodiac, Hush and CIDCO. Having worked within both EMEA and APAC teams, I call myself an international marketer. I 've been active in the Middle East region for the past couple of years through two of the companies I have worked with. Currently, I manage marketing, demand generation and PR in my current role and overall, I have been part of the larger domain of marketing which includes advertising, PR, event management, digital and social media

marketing. One of my campaigns has also won the CLIO silver award in the past. I was also awarded the Omron Global Awards during my tenure at Omron.

What, in your opinion, are some of the toughest challenges facing a marketing professional?

In my opinion, the toughest challenges marketing professionals are facing today is to keep up with latest trends in digital marketing, MarTech and marketing automation. With the emergence of generative AI in marketing domain, this space is expected to evolve and advance at a very fast pace and balancing oneself as a marketer in this scenario can be a challenge for a lot of marketing professionals. On the flip side, this seems to be more of a growth opportunity rather than a challenge.

How do you cope with the stresses and demands of the job? What's your mantra for success is ?

I think keeping calm and focusing on the job without any distractions is the way to go. My mantra for success is to be strong

at basics of marketing and evolve time to time with latest trends. Being positive and having a go-getter attitude with the right communication skills, is key to success.

What's your idea of an ideal weekend?

My ideal weekend should be an easy mix of a little laziness to begin with, some delicious food, good outings and quality time with family and friends. This is good enough to recharge oneself for the coming week.

What advice would you give to budding, young marketing professionals/ aspirants?

My advice is simple. Define your goals and identify your target audience and channels to achieve these. Always be positive and keep going. Being a marketer, the first thing you have to market is yourself. Identify your target audience, communication channels and position yourself. Focus on marketing basics and keep up with the latest trends in marketing. Upgrade your marketing skills continuously.

ESET RESEARCH DISCOVERS NEW CYBERESPIONAGE GROUP

SET Research has discovered a new cyberespionage group, MoustachedBouncer. It is named after its presence

in Belarus and is aligned with the interests of the local government. Active since at least 2014, the group targets only foreign embassies, including European ones, in Belarus. Since 2020, MoustachedBouncer has most likely been able to perform adversary-in-themiddle (AitM) attacks at the ISP level, within Belarus, in order to compromise its targets. The group uses two separate toolsets that ESET has named NightClub and Disco. The research was exclusively presented during the Black Hat USA 2023 conference on August 10, 2023, by ESET researcher Matthieu Faou.

According to ESET telemetry, the group targets foreign embassies in Belarus, and ESET has identified four countries whose embassy staff have been targeted: two from Europe, one from South Asia, and one from Africa. ESET assesses that MoustachedBouncer is very likely aligned with Belarus interests and specializes in espionage, specifically against foreign embassies in Belarus. MoustachedBouncer uses advanced techniques for Command and Control (C&C) communications, including network interception at the ISP level for the Disco implant, emails for the NightClub implant, and DNS in one of the NightClub plugins.

While ESET Research tracks MoustachedBouncer as a separate group, we have found elements that



make ESET assess with low confidence that it is collaborating with another active espionage group, Winter Vivern, which has targeted government staff of several European countries, including Poland and Ukraine, in 2023.

To compromise their targets, MoustachedBouncer operators tamper with their victims' internet access, probably at the ISP level, to make Windows believe it's behind a captive portal. For IP ranges targeted by MoustachedBouncer, network traffic is redirected to a seemingly legitimate, but fake, Windows Update page," says ESET researcher Matthieu Faou, who discovered the new threat group. "This adversary-in-the-middle technique occurs only against a few selected organisations, perhaps just embassies, not countrywide. The AitM scenario reminds us of the Turla and StrongPity

threat actors, who have trojanised software installers on the fly at the ISP level."

"While the compromise of routers in order to conduct AitM attacks on embassy networks cannot be fully discarded, the presence of lawful interception capabilities in Belarus suggests the traffic mangling is happening at the ISP level rather than on the targets' routers," explains the ESET researcher.

"The main takeaway is that organisations in foreign countries where the internet cannot be trusted should use an end-to-end encrypted VPN tunnel to a trusted location for all their internet traffic in order to circumvent any network inspection devices. They should also use topquality, updated computer security software," advises Faou. **1**

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



< nuclias

cloud

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







SIMPLE. POWERFUL. SECURE.

The unified platform for digital transformation.

- Enable autonomous operations.
- Control costs and complexity.
- Increase agility and productivity.

solarwinds.com



