

Security

ADVISOR

MIDDLE EAST

INNOVATING CYBER DEFENCE

NICOLAI SOLLING, CHIEF TECHNOLOGY OFFICER AT HELP AG TELLS ANITA JOSEPH HOW THE COMPANY'S INNOVATION-FIRST APPROACH AND SKILL BUILDING INITIATIVES HAVE CONSOLIDATED ITS POSITION AS THE CYBERSECURITY FRONTRUNNER IN THE REGION.



TryMe™
Scan to experience



Keep an eye on your home from anywhere

Video doorbells, security cameras and alarm system

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

Ring... smart security for every home.



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

Available at:

Dubai	MYZ	DSR Tech	AL Ershad	Hyper X	Innox	AI Muhairi General Trading LLC
	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 4 393 2107
Abu Dhabi	Royal Phone Center	Empower / Apple Plus Computers	Asia Mobile Palace			
	Tel: +971 2 491 8888	Tel: +971 2 445 3222	Tel: +971 55 652 3400			



12 INNOVATING CYBER DEFENCE



6 News from the cybersecurity industry in the region and beyond.

38 Dave Russell, Vice President, Enterprise Strategy at Veeam, on the evolution of Zero Trust.

28 Wesley Wang, Director of Channel Development & MarCom at Hikvision MEA, on the company's innovation-first approach and its plans for the region for 2024.

42 Meriam El Ouazzani, Regional Director - Middle East, Turkey, Africa at SentinelOne, on why energy and utility sectors Continue to be targeted by threat actors.



Secure Your **Digital Future**

Simple. Secure. Resilient.



**Secure Your Enterprise IT Footprint
For A Safer Digital Journey**

www.raqmiyat.com

UAE | KSA | INDIA

EDITOR'S NOTE



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

Anita Joseph
Editor

INVESTING IN SKILLS

In an era dominated by technological advancements and an ever-expanding digital landscape, the importance of cybersecurity cannot be overstated. As we delve into the intricate world of digital threats, one glaring concern surfaces—the widening gap in cybersecurity skills. The relentless evolution of cyber threats necessitates a workforce equipped with the right skills to defend against these ever-changing dangers.

The cybersecurity skills gap has become a pressing issue, with organisations struggling to find and retain qualified professionals to safeguard their digital assets. The demand for cybersecurity expertise far exceeds the current supply, leaving organisations vulnerable to increasingly sophisticated cyber-attacks. This deficit not only poses a threat to individual companies but also has broader implications for global security.

Amidst this challenge, the concept of cyber immunity emerges as a vital aspect of security. Cyber immunity refers to an organisation's ability to withstand, adapt

to, and recover from cyber threats, akin to the immune system's role in protecting the human body from diseases. Building cyber immunity requires a multifaceted approach that combines advanced technology, strategic planning and most importantly, a skilled workforce.

Organisations must prioritise collaboration with educational institutions, industry partners, and government agencies to establish pipelines for cybersecurity talent.

NURTURING THE NEXT GENERATION

Internship programs, mentorship initiatives, and apprenticeships can help bridge the gap between theoretical knowledge and practical skills, nurturing the next generation of cybersecurity experts.

As we navigate the intricate challenges of the digital age, the pursuit of cyber immunity becomes a collective responsibility. By addressing the cybersecurity skills gap through education, training, and collaboration, we can fortify our defenses and create a resilient digital ecosystem capable of withstanding the ever-growing array of cyber threats.

EVENTS



FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by **CPI**

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

EDITORIAL
Editor
Anita Joseph
anita.joseph@cpimediagroup.com

PRODUCTION AND DESIGN
Designer
Prajith Payyapilly
prajith.payyapilly@cpimediagroup.com

DIGITAL SERVICES
Web Developer
Adarsh Snehan
webmaster@cpimediagroup.com

Publication licensed by
Dubai Production City, DCCA
PO Box 13700
Dubai, UAE

Tel: +971 4 5682993

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

© Copyright 2024 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.

CISCO UNVEILS INNOVATIONS ON THE CISCO OBSERVABILITY PLATFORM

Cisco has announced a series of exciting

new solutions — enriched by business context — on the Cisco Observability Platform. With applications acting as the front door for nearly every business — and delivering a flawless application experience a top priority for IT teams — the latest enhancements will help customers deliver secure and performant user and application experience.

With application experience expectations at an all-time high, technologists can now leverage new Digital Experience Monitoring (DEM) capabilities for both hybrid and cloud environments. The new DEM application includes Real User Monitoring (RUM) and Session Replay modules for deep insights into browser and mobile applications performance and efficient resolution of session-level issues. In addition, integrations with Cisco ThousandEyes and Cisco Accedian empower applications and network teams with the insights into service delivery required to identify whether the root cause of impacted digital experience is the application, network or cloud infrastructure.

Cisco offers observability for Kubernetes workloads on the Cisco



Observability Platform, using the powerful, lightweight Linux kernel utility, extended Berkeley Packet Filters (eBPF). Operating at the kernel level allows operators access to granular visibility into network activity, resource utilisation, application dependencies and misconfigurations impacting network performance, without the need for multiple tools, cross-team collaboration and manual dependency mapping.

Cisco is delivering a unified experience

across its observability portfolio, with new capabilities across Cisco AppDynamics and the Cisco Observability Platform. Using a single account and shared context, the unified observability experience arms operators with capabilities including Log Analytics, to search with context and improved log storage; and Core Web Vitals, providing front-end application owners the golden signals to keep their web pages from being de-ranked for poor user experience.

SAS TRAINS SAUDI BANKERS ON BUILDING INTELLIGENT CREDIT RISK SCORECARDS

SAS, the leader in analytics, has

successfully hosted a “Credit Scorecard Development and Implementation” in-person class in Riyadh, highlighting the significance of cultivating a risk-aware culture in Saudi Arabia’s banking industry. The session was held on January 31st and February 1st, 2024, at the Hilton Riyadh Hotel & Residences.

A thriving financial sector is recognised as an essential facilitator in the realisation of the ambitious goals outlined in the Saudi Vision 2030. As per the projections of the Financial Sector Development Program, the sector is

anticipated to reach a large enough size by 2030 to fund large-scale projects, offer a diverse set of traditional and innovative products and services, give previously excluded citizens access to the financial system through an inclusive structure, achieve a high degree of digitisation, and uphold financial stability. However, with the constantly evolving Saudi Arabian financial landscape, the credit risk that financial institutions take on has changed in terms of scale, complexity, and nature. Thus, robust credit risk management has to be an integral component of

the long-term viability of any financial institution.

No matter how a financial institution prioritises risk, SAS has proven methodologies and best practices to help establish a risk-aware culture, optimise capital and liquidity, and meet regulatory demands. Bringing credit risk and scoring managers, data miners, professionals involved in model vetting, validation and auditing, risk strategy developers, and credit risk executives under one roof, SAS provided participants with an in-depth training session to enable risk modelers to build intelligent scorecards.

COMMSCOPE UNVEILS SYSTIMAX 2.0 PROVIDING INNOVATIVE SOLUTIONS TO ADDRESS NETWORK INFRASTRUCTURE CHALLENGES

CommScope, a global leader in network connectivity, has announced SYSTIMAX 2.0 enhancements, the next generation of its SYSTIMAX building and data center connectivity portfolio which provides customers with the latest structured cabling solutions and support to meet the challenges of today and tomorrow.

Inside buildings, data centers and across campuses, technology disruption and operational demands are intensifying. Therefore, it's more important than ever to deploy an agile, dependable and future-ready infrastructure. For nearly 40 years, SYSTIMAX solutions have led the

trajectory of tomorrow's network technologies, supporting customers' network evolution within a fluid business environment. As the trusted solution in structured cabling, SYSTIMAX technology has been synonymous with exceeding the standards of enterprise connectivity, continuously evolving to redefine how building, data center and campus networks operate. SYSTIMAX 2.0 enhancements carry that legacy forward, leveraging CommScope's rich history of performance and reliability in copper, fiber and network intelligence.

"With the SYSTIMAX 2.0 enhancements, CommScope is expanding its support for



future customer needs with continuous technology innovation, world-class performance and reliability, application assurance and unrivaled global support," stated Luc Adriaenssens, VP of Enterprise Product Management and R&D, CommScope. "We will be evolving the SYSTIMAX portfolio of products and services to ensure we continue to meet those needs."

PURE STORAGE SOLUTION RECEIVES STAC-M3 BENCHMARK FOR HIGH-PERFORMANCE AND QUANTITATIVE TRADING

Pure Storage, the IT

pioneer that delivers the world's most advanced data storage technology and services, announced that its FlashBlade//S500 has achieved the STAC-M3 Benchmark, an industry standard for tick-analytics benchmarks, specifically designed for database software/hardware stacks managing large time series of market data.

The benchmarked system featured FlashBlade//S500, a purpose-built, all-QLC flash, unified fast file and object (UFFO) storage platform. 13 of 17 STAC-M3 Antuco (baseline) mean-response time benchmarks witnessed improvements while 17 of 24 STAC-M3 Kanaga (scaling) mean-response time benchmarks exhibited enhancements. Additionally, when compared to a cloud-based solution, Pure Storage



FlashBlade//S500 outperformed in 9 of 17 Antuco benchmarks and 12 of 24 Kanaga benchmarks, showcasing significant speed advantages.

These results validate the FlashBlade//S500 series' performance. FlashBlade is designed to deliver exceptional performance, throughput, and continuous uptime — critical requirements for data scientists and quantitative analysts running multi-threaded, time-series workloads. The platform enables firms to run complex queries across data sets of any scale with maximum throughput

and minimum latency. As workloads increased in volume and thread count, Pure Storage FlashBlade//S500 demonstrated the ability to handle highly parallel workloads efficiently. The architecture allowed for seamless scalability, crucial for the

demanding requirements of quant and high-frequency trading.

Commenting on the results, Jack Gidding, CEO of STAC, said "We are pleased to welcome Pure Storage to the ranks of technology providers who submit solutions for independent testing against the customer-developed STAC Benchmark standards. Financial firms on the STAC Benchmark Council designed STAC-M3 to test a representative range of business use cases, and the need for fast and efficient time-series analysis has never been higher."

ESET RESEARCH DISCOVERS ESPIONAGE APPS ON THE ATTACK IN PAKISTAN, UTILIZING ROMANCE SCAMS

ESET researchers have identified 12 Android espionage apps that share the same malicious code; six were available on Google Play. All the observed applications were advertised as messaging tools, apart from one that posed as a news app. In the background, these apps covertly execute remote access trojan (RAT) code called VajraSpy, used for targeted espionage by the Patchwork APT group. The campaign mostly targeted users in Pakistan. Based on ESET's investigation, the threat actors behind the trojanised apps probably used a honey-trap romance scam to lure their victims into installing the malware.

VajraSpy has a range of espionage functionalities that can be expanded based on the permissions granted to the app bundled with its code. It steals contacts, files, call logs, and SMS messages, but some of its

implementations can even extract WhatsApp and Signal messages, record phone calls, and take pictures with the camera.

Based on available numbers, the malicious apps that used to be available on Google Play were downloaded more than 1,400 times. During the ESET investigation, weak operational security of one of the apps led to some victim data being exposed, which allowed researchers to geolocate 148 compromised devices in Pakistan and India. These were likely the actual targets of the attacks. ESET is a member of the App Defense Alliance and an active partner in the malware mitigation program, which aims to quickly find Potentially Harmful Applications and stop them before they ever make it onto Google Play. As a Google App Defense Alliance partner,



ESET identified the malicious apps and reported them to Google, and they are no longer available on the Play store. However, the apps are still available on alternative app stores.

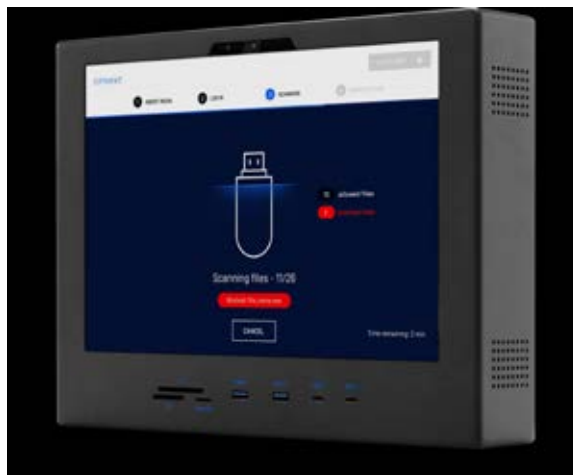
Last year, ESET detected a trojanised news app called Rafaqat being used to steal user information. Further research has uncovered several more applications with the same malicious code. In total, ESET analysed 12 trojanised apps, six of which (including Rafaqat) had been available on Google Play, and six found in the wild – in the VirusTotal database.

OPSWAT LAUNCHES INNOVATIVE ENHANCEMENTS TO ITS METADEFENDER KIOSK SERIES

OPSWAT, a leader in critical infrastructure protection (CIP) cybersecurity solutions, is proud to announce new advancements to its MetaDefender Kiosk product line.

In response to the escalating challenges faced by organisations in managing and handling threats originating from peripheral media such as USBs and bring-your-own-devices (BYOD), OPSWAT continues its commitment to innovation. The MetaDefender Kiosk is a testament to this, providing a solution for securing critical environments – now with even better options for customers.

"These product enhancements mark a significant step forward in the evolution of OPSWAT's MetaDefender Kiosk product line, addressing the dynamic challenges



faced by organisations in securing critical environments," said Benny Czarny, Founder and CEO at OPSWAT. "The Kiosk Mini, Kiosk Stand, and first-of-its-kind integration with MetaDefender Sandbox and Media Firewall technologies, redefine

accessibility and functionality, setting a new standard for OT cybersecurity."

A unique addition to the entire MetaDefender Kiosk product line is the integration with OPSWAT's Sandbox technology – the first peripheral media scanning solution in the industry that enables adaptive threat analysis technology for zero-day malware detection, even in air-gapped areas without the installation of software on critical assets. Additionally, integration with MetaDefender Media Firewall enables policy enforcement with a no-touch solution and zero endpoint installation. With this, OPSWAT enables defense-in-depth peripheral media protection for critical environments.



معرض و مؤتمر الخليج العالمي لأمن المعلومات

GISEC

GLOBAL

23-25 APR 2024
DUBAI WORLD TRADE CENTRE

A BOLD NEW FUTURE

AI-DRIVEN CYBER RESILIENCE

THE **SUPER CONNECTOR** EVENT FOR THE MIDDLE EAST & AFRICA'S **CYBERSECURITY COMMUNITY**

GET INVOLVED

gisec@dwtc.com | Tel: +971 4 308 6469

SCAN HERE



#gisecglobal | gisec.ae

HOSTED BY

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

OFFICIAL GOVERNMENT
CYBERSECURITY PARTNER

مركز الأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

OFFICIALLY SUPPORTED BY



شرطة دبي
DUBAI POLICE

OFFICIAL
DISTRIBUTION PARTNER

SPIRE
SPECIAL INVESTIGATION & PROTECTION

LEAD STRATEGIC
PARTNER

HUAWEI

STRATEGIC
PARTNER



PLATINUM
SPONSOR

PENTERA

GOLD SPONSOR

CLOUDFLARE

**MENLO
SECURITY**

NOKIA

Qualys

BRONZE SPONSOR

Honeywell

sekoia



UAE & KSA AHEAD OF GLOBAL COUNTERPARTS IN BLOCKING FRAUDULENT EMAILS

As Google, Yahoo! and Apple prepare to roll out new email authentication requirements designed to prevent threat actors from abusing email, research from leading cybersecurity and compliance company Proofpoint reveals that organisations in the UAE and KSA are more prepared with their email security best practices than global counterparts. According to a DMARC (Domain-based Message Authentication, Reporting, and Conformance) analysis of the Forbes Global 2000 companies, a majority of organisations in the UAE (80%) and KSA (90%) have published a DMARC record, compared to just 73% of the overall global listed companies.

DMARC is an email validation protocol designed to protect domain names from being misused by cybercriminals, decreasing impersonation risk for brands. It authenticates the sender's identity before allowing the message to reach its intended designation. 'Reject' is the strictest and recommended level of DMARC protection, a setting and policy that blocks fraudulent emails from reaching their intended target.

As both Google and Yahoo! have

announced that email authentication will need to be in place when sending messages to their respective accounts during the first quarter of this year, bulk senders will have even more email authentication requirements to meet, including having a robust DMARC policy in place.

"Countries in the GCC, especially the UAE and KSA, are continually improving their cyber preparedness, but they must continue to improve measures against fraudulent communication attempts via the number one threat vector – email. Cybercriminals regularly use the method of domain spoofing to pose as well-known organisations and companies by sending an email from a supposedly legitimate sender address. These emails

are designed to trick people into clicking on links or sharing personal details, which can then be used to steal money or identities," says Emile Abou Saleh, Senior Director for Middle East, Turkey, and Africa at Proofpoint. "It can be almost impossible for an ordinary Internet user to identify a fake sender from a real one. By implementing the strictest level of DMARC – "reject" – organisations can actively block fraudulent emails from reaching their intended targets, protecting their customers, partners, and suppliers from cyber criminals looking to impersonate their brand."

"Even as leading organisations adopt critical measures to prevent threat actors from sending malicious emails to targets, they will need to move quickly to comply with the new Google and Yahoo! email authentication requirements," said Emile Abou Saleh, Senior Director for Middle East, Turkey and Africa at Proofpoint. "Companies that send to Gmail or Yahoo! must have Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) authentication methods implemented, as well as a DMARC policy in place." 📧

**CYBERCRIMINALS
REGULARLY USE THE
METHOD OF DOMAIN
SPOOFING TO POSE
AS WELL-KNOWN
ORGANISATIONS,
PROOFPPOINT REVEALS**

INNOVATING CYBER DEFENCE

Nicolai Solling is Chief Technology Officer at Help AG where he oversees the company's professional and support services, along with managing technical vendor relationships across the region. With a rich career history spanning over two decades in the IT and network industry, Nicolai plays a pivotal role in designing, deploying and operating complex network and security infrastructure for enterprise clients in diverse sectors. Renowned for his cybersecurity acumen, Nicolai is a coffee enthusiast who finds himself captivated by the boundless possibilities of technology. His hands-on experience and extensive know-how in areas such as security solutions, integration, presales, and design, consolidate his reputation as one of the industry's well-respected leaders.

Anita Joseph, Editor at Security Advisor Middle East, meets Nicolai for a candid chat on Help AG's commitment to innovation, technology integration and bridging the security skills gap.

Commitment to Continuous Innovation

Right at the outset, Nicolai sets the tone of the conversation with one word: Innovation. As a company that has innovation deeply embedded in its DNA, Help AG is the undisputed gamechanger in the industry, disrupting the market with its cutting-edge solutions and cybersecurity expertise.

"The company is built around the core principle of providing clients with cutting-edge solutions, technology services, and innovative approaches. From its inception, Help AG has had innovation at its heart, and been at the forefront of introducing groundbreaking technologies to the market. We are deeply committed to technological and solution innovation, constantly striving to address the evolving challenges faced by our customers. Our approach involves a continuous effort to comprehend the specific challenges customers encounter, leading us to innovate and enhance our services and capabilities accordingly," he points out.

Harnessing the Power of AI

Reinforcing this journey of innovation, Nicolai delves into the role of Artificial Intelligence (AI) in today's cybersecurity landscape. He highlights the role of AI, evolving from safeguarding sensitive data in AI platforms to addressing challenges posed by generative AI models.

"AI is a prominent area of focus for our clients, who are also keenly interested in its deployment within their organisations. A year ago, the primary concern around AI revolved around preventing the inadvertent leakage of sensitive data into AI platforms. This marked the initial step in the realm of generative AI, where experimentation often involved inputting various information into GPT prompts. Therefore, addressing the challenge of how data



integrates into AI models became a focal point of our efforts, collaborating closely with clients to find effective solutions,” he says.

“However, the landscape is evolving rapidly. Clients are now actively constructing their generative AI models, exposing them to end-users in different forms, such as chatbots. This shift brings forth new considerations, particularly regarding the control of information emanating from these chatbots, especially when trained on extensive enterprise data. So then, ensuring the secure utilisation of AI becomes paramount. Additionally, we are navigating the intricacies of where AI models reside, marking a pivotal area for innovation in our services and solutions. The quest is to identify the next generation of cybersecurity solutions poised to enter the market.”

Going Beyond the Conventional

Help AG’s innovation-centric approach extends beyond conventional cybersecurity realms. Nicolai discusses the importance of innovation in areas like Cloud and Application Security, operational technology (OT), and Internet of Things (IoT) Security, identity and access management and data protection and privacy. “As organisations embark on their digital transformation journey and adopt more technologies such as the cloud, operational technology, and others, Help AG aims to support them in navigating the complexities of modern cybersecurity threats.”

“For Help AG, cloud security extends beyond conventional boundaries. While our focus aligns with the term ‘cloud security’ used by our customers, our efforts delve deeper into securing modern applications. As organisations modernise their applications in the cloud, we prioritise fortifying their security posture. Our approach integrates DevSecOps principles, emphasising proactive measures to secure applications early in the development lifecycle. Thus, our commitment lies in

safeguarding modern applications within the cloud environment, ensuring our customers’ digital assets remain resilient and future-ready.”

Another pivotal area of innovation pertains to identity security. “Identity serves as a foundational pillar for any organisation, dictating access rights to systems and data. In the contemporary cybersecurity landscape, the concept of identity is arguably the most critical. Systems housing identity information are inherently vulnerable due to their crucial role. In the context of digital transformation, access to identity services becomes as essential as having access to clean drinking water. The availability and security of these services thus become paramount.”

Nicolai also says understanding the significance of identities is imperative, considering that attackers require privileges and access within a network. “The control of such privileges lies within the realm of identity solutions. Consequently, robust capabilities in securing identity services not only safeguard an organisation but also provide a means to mitigate a substantial portion of daily cyber threats. Engaging with customers, I dedicate considerable time to discussions on implementing effective identity security measures, identifying and advocating for innovative solutions. Within our Cyber Defence Centre, many monitored use cases are centered around these critical identity components, recognising them as the Achilles heel of contemporary cybersecurity.”

Staying Ahead of Escalating Cyber threats

In today’s ever-evolving digital landscape, cyber threats are on the rise, becoming

more and more sophisticated with time. One of the most prominent threats in the region and globally is Distributed Denial of Service (DDoS) attacks.

“DDoS poses a significant and persistent challenge in the realm of online business,” says Nicolai. “It has become an inherent cost that organisations must bear when conducting operations on the internet due to the constant threat of DDoS attacks. The trend over the past years reveals a concerning escalation, both in the frequency and magnitude of these attacks. Each passing year surpasses the previous one in terms of the number and size of DDoS attacks.”

In 2023, Help AG’s DDoS infrastructure detected an astounding count of over 200,000 DDoS attacks, marking a significant increase from the previous year’s tally of 150,000. “Notably, the latter part of the year, specifically November and December, witnessed a substantial surge in DDoS incidents. The motives behind these attacks are often linked to cybercriminal speculation, strategic timing around high-profile events and other similar considerations.”

According to Nicolai, a noteworthy technical shift in DDoS attack patterns is seen in the increased utilisation of encrypted traffic by attackers. “Historically, encrypted traffic was not a prevalent component of DDoS attacks due to the computational challenges faced by attackers in creating encrypted tunnels. However, this obstacle seems to have been overcome, introducing a new set of tools employed by attackers. Consequently, our defensive measures must evolve to address these changing tactics.”

Therefore, in advising clients and disseminating advisories, Help AG

HELP AG’S ADVANTAGE OF SCALE ALLOWS FOR EFFICIENT AND WIDESPREAD DELIVERY OF CYBERSECURITY SOLUTIONS AND SERVICES TAILORED TO DIVERSE CLIENT NEEDS.

emphasises the importance of adopting a comprehensive DDoS defence strategy. “While network-level defence remains a forte, we stress the need to extend protection to the application layer. Modern DDoS attacks, some of which generate minimal traffic bypassing traditional detection methods that look for sudden spikes in traffic, have shifted from targeting network bandwidth to exploiting application vulnerabilities. Achieving a balance between safeguarding both the application and infrastructure with a multi-layered defence strategy is imperative to effectively combat the evolving nature of DDoS attacks” Nicolai stresses.

Enter Automation

As automation takes centerstage in today’s cybersecurity landscape,

HELP AG IS CONTINUOUSLY AIMING TO CREATE A STRONG CYBERSECURITY CULTURE BOTH INSIDE THE COMPANY AND IN ALL THEIR CUSTOMER ORGANISATIONS.

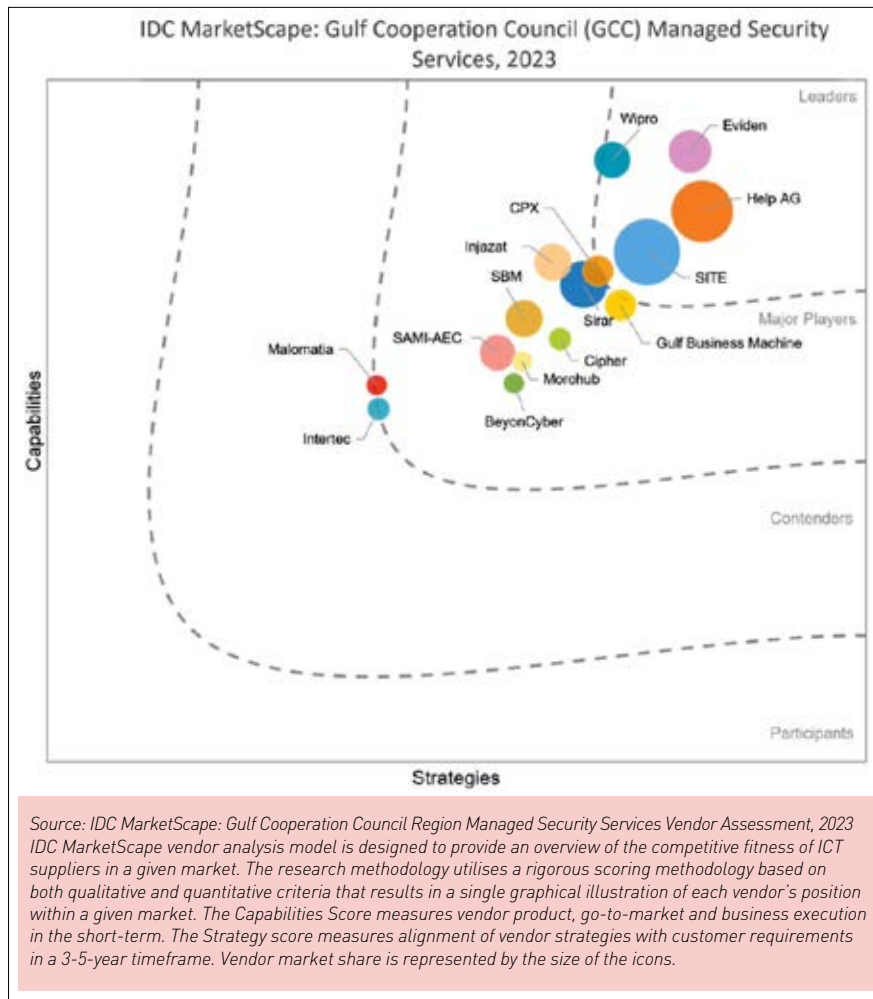
Help AG stands tall, well-equipped to seamlessly integrate it into its technology and processes. In Nicolai’s words: “Automation plays a crucial role, especially in advanced defence against cyber threats. Automation can detect and respond to threats much faster than human teams, which is crucial given the rapid pace at which many cyber-attacks unfold, particularly because the shortened dwell time for attackers necessitates a swift and automated response. Recognising this, we made a strategic

decision at Help AG two years ago, to integrate automation into every client environment we deploy. Each new client receives a set of automation use cases from day one, progressively enhancing the robustness of their response over time. Automation is a central discipline for us, and significant engineering efforts are dedicated to its development.”

Help AG’s Cyber Defence Centre comprises over 170 security experts, with the cyber engineering team being the largest. They focus on ensuring the seamless operation of their automation platform and meticulously construct use cases for integration into diverse systems, incorporating programming, scripting, and API integrations. Meanwhile, the analysts in the team play a pivotal role in identifying different issues and possibilities. This collaboration means that Help AG is able to enhance its automated responses based on potential scenarios.

“While analysts form the backbone of our service, empowering them with the right automation tools transforms the team into a dream unit,” Nicolai says. “Our ultimate goal is to simplify their work, facilitate quicker decision-making through automation and create a highly effective cybersecurity defence mechanism.”

With its investment in intelligent automation and its service-oriented architecture, Help AG offers customers 360-degree visibility into multiple aspects of their managed security services. This investment, combined with the company’s long history of providing managed security services in the region, has earned Help AG the title of Managed Security Services Leader in the GCC by IDC MarketScape in 2023.





Cybersecurity as a Service

Nicolai makes the insightful assertion that most organisations find it inherently challenging to manage their own cybersecurity needs, mainly because this falls outside their core area(s) of expertise, and this is where Help AG steps in with Cybersecurity as a Service, to ensure a seamless and easy journey for its customers.

"For many organisations, cybersecurity is not a primary area of expertise and may be outside their usual scope. For such entities, attempting to establish in-house incident response and cyber defence services can be well beyond the normal comfort zone. Recognising

AUTOMATION IS A CENTRAL DISCIPLINE FOR US, AND SIGNIFICANT ENGINEERING EFFORTS ARE DEDICATED TO ITS DEVELOPMENT.

this, organisations are increasingly turning to external expert managed service providers like Help AG to handle the complexities of cybersecurity services. This collaboration allows them to offload responsibilities, whether in monitoring cybersecurity events, conducting dark web investigations, or ensuring comprehensive vulnerability assessments and external attack surface management. These capabilities are critical but demand operational procedures, engineering expertise, and diligent follow-up-areas where we excel in supporting our customers.”

“It’s essential to clarify that, while customers retain ultimate responsibility for their cybersecurity, our partnership enhances their response capabilities significantly. By working hand in hand, we provide a comprehensive and effective approach to cybersecurity, enabling organisations to focus on their core competencies while ensuring a robust defence against evolving threats” he adds.

Help AG’s suite of cybersecurity services not only pioneers innovative solutions but is also rigorously designed to meet and exceed local and global compliance standards, in the UAE and KSA. This steadfast commitment positions Help AG as the preferred partner for enterprises and government entities, especially within critical sectors where the integrity and security of data are paramount.

“By choosing us, stakeholders can rest assured that they are not only leveraging cutting-edge cybersecurity technology but are also aligning with a partner whose operations are synonymous with excellence and compliance at every level” says Nicolai.

Economy of Scale

Help AG’s advantage of scale allows for efficient and widespread delivery of cybersecurity solutions and services tailored to diverse client needs. Their approach to delivering exceptional

BY WORKING HAND IN HAND, WE PROVIDE A COMPREHENSIVE AND EFFECTIVE APPROACH TO CYBERSECURITY, ENABLING ORGANISATIONS TO FOCUS ON THEIR CORE COMPETENCIES WHILE ENSURING A ROBUST DEFENCE AGAINST EVOLVING THREATS.

client solutions is anchored in strategic partnerships and the sophisticated use of automation. “By collaborating with key industry vendors and being active members on partner advisory boards, we ensure that our solutions are not just cutting-edge but also meticulously tailored to meet our clients’ unique requirements. Our partnerships are chosen with precision, aiming for optimal outcomes through a blend of comprehensive engineering and integration,” says Nicolai.

“The heart of our service delivery philosophy lies in automation. It’s our belief that scalability and efficiency in deploying updates and solutions are paramount. Automation stands as the cornerstone of this belief, enabling us to offer seamless processes that allow for the deployment of updates at the touch of a button—a feat impractical to achieve manually. This focus on automation and scalability underscores the importance we place on evolving service delivery, highlighting how we adapt to meet the dynamic needs of our diverse clientele through technology.

“Furthermore, our engagement in co-innovation and co-creation of cybersecurity solutions with industry-leading vendors ensures that we remain at the cutting edge of protecting against today’s threats and anticipating those of tomorrow. Our dedication to innovation, in partnership with global cybersecurity leaders, affirms our position as a forward-thinking ally for any organisation navigating the complexities of the digital age.”

Bridging the Gap

Nicolai highlights Help AG’s efforts in bridging the cybersecurity skills gap in today’s ecosystem. He mentions how initiatives like Help AG’s MSS Graduate Program and academia partnerships reinforce the company’s commitment to nurturing cybersecurity talent.

“One of the biggest concerns of organisations worldwide is the gap in cybersecurity skills. Today, there is a big difference between the cybersecurity needs of organisations and the availability of professionals with the required skills to fill these needs. Help AG is committed to bridging this gap and I think it’s important that we as a society become more secure and create a better ecosystem around cybersecurity. We recently launched our MSS Graduate Program, where we provide fresh graduates with a six-month training in cybersecurity. We have six graduates that are going through the programme. I hope we can absorb them into the company once they’ve done with the programme and offer them a good starting point in their career where they can learn from experts in the field.”

In addition, Help AG is continuously aiming to create a strong cybersecurity culture both inside the company and in all their customer organisations – an environment where employees are engaged, motivated, and feel that their contributions are making a difference, to build a stronger, more resilient cybersecurity workforce that can meet the challenges of today and tomorrow.

Fostering Awareness and Education in Cybersecurity

Nicolai highlights another gap that Help AG is working on closing in cybersecurity, the awareness gap. Efforts to engage individuals and organisations in discussions about cybersecurity challenges and solutions play a crucial role in enhancing the collective understanding and resilience against cyber threats.

On this matter, Nicolai says “We address the awareness gap among customers by focusing on problem discussions, hosting free events on crucial topics like identity governance and OT security. Our approach is about raising awareness of industry challenges. Additionally, I prioritise understanding and addressing current and future client problems by collaborating with academia and regulatory bodies, to prepare for crucial client engagements and solution development in the near term. We also engage with mainstream and business media to discuss widespread cybersecurity challenges, and present information in an accessible manner to the public.”

The e& Ecosystem

Present in the Middle East since 2004, Help AG was strategically acquired by e& (formerly Etisalat Group) in 2020, to become the cybersecurity arm of e& enterprise.

“As a proud member of the e& ecosystem, Help AG stands at the forefront of technological

innovation and investment. e& enterprise encompasses a broad spectrum of digital transformation capabilities including cloud services, cybersecurity, artificial intelligence (AI), Internet of Things (IoT), fintech, and blockchain technologies. This not only amplifies our capabilities but also enriches our offerings, allowing us to deliver comprehensive solutions to enterprises and governments,” Nicolai comments.

“Being part of this ecosystem positions us uniquely in the market. It enables us to leverage the economy of scale inherent within a vast, interconnected group. This synergy ensures that Help AG can offer a non-parallel value proposition, blending cutting-edge technology with strategic insights to serve as an invaluable partner for organisations embarking on their digital transformation journey”.

The Road Ahead

The future is clear for Help AG: Continue to innovate, adapt, and integrate cutting-edge technology, particularly AI and intelligent automation, post quantum cybersecurity and the use of sustainable tech in the realm of cyber.

“Our focus will delve extensively into the realm of securing AI, presenting both innovative service and technological advancements. Internally, we’re engaged in AI projects, exploring the integration of AI and machine learning for various initiatives. Additionally, we assist customers in implementing AI capabilities within their security

platforms, aiding in their management and operation. The landscape of AI is broad, encompassing aspects of prevention and operational efficiency. Another key area is quantum computing, where we’re aiming to deepen our understanding of client needs and create solutions that will ease their challenges. A pivotal aspect of our strategy involves streamlining operations with intelligent automation, particularly within our Cyber Defence Centre. Ultimately, our goal is to reach a level of confidence in automation that extends to automatic responses, differentiating between routine automation and proactive responses tailored to specific incident outcomes.

Investments in engineering and platform capabilities are crucial to support these initiatives. Where existing platforms fall short, we develop custom automation solutions to meet customer requirements, leveraging our expertise to generate innovative ideas and solutions.”

Conclusion

Help AG stands at the forefront of the technological landscape, embodying an unwavering commitment to innovation that shapes the future of cyber resilience in the region. The company’s dedication to pushing technological boundaries is evident in its adept innovation and integration of cutting-edge solutions to meet industry requirements.

Through strategic initiatives, the company facilitates a symbiotic relationship that ensures technology serves as an enabler for both corporate success and societal progress. This holistic approach underscores Help AG’s commitment to responsible and inclusive innovation.

As it continues to evolve within the dynamic digital landscape, its resilience and forward-thinking strategies are evident. Help AG’s journey goes beyond defending against emerging threats, it involves

THIS SYNERGY ENSURES THAT HELP AG CAN OFFER A NON-PARALLEL VALUE PROPOSITION, BLENDING CUTTING-EDGE TECHNOLOGY WITH STRATEGIC INSIGHTS TO SERVE AS AN INVALUABLE PARTNER FOR ORGANISATIONS EMBARKING ON THEIR DIGITAL TRANSFORMATION JOURNEY.



**OUR DEDICATION
TO INNOVATION,
IN PARTNERSHIP
WITH GLOBAL
CYBERSECURITY
LEADERS, AFFIRMS
→ OUR POSITION
AS A FORWARD-
THINKING ALLY FOR
ANY ORGANISATION
NAVIGATING THE
COMPLEXITIES OF THE
DIGITAL AGE.**

innovating to equip organisations with the means to build proactive defences and the agility to predict and adapt to new threats. This commitment to innovation enhances the synergy of people, processes, and technologies, offering the best in security solutions. In essence, with a philosophy of Innovate. Automate. Elevate., Help AG is committed to INNOVATE processes and technologies, AUTOMATE threat detection, and response playbooks for faster time to value, in order to ultimately ELEVATE the resilience of organisations in an era that demands utmost agility and performance every single day. Help AG is not just an information technology provider; it is a catalyst for positive change, a bridge connecting the aspirations of industries with the needs of the public and a trailblazer in embracing AI and emerging technologies. Through its unwavering commitment to innovation and technological integration, Help AG cements its position as a leader in shaping the digital landscape of tomorrow. 🔑

MICROSOFT UAE HOSTS 'BUILD: AI DAY' TO ACCELERATE AI INNOVATION

Microsoft UAE has announced its 'Microsoft Build: AI Day' tour in UAE. The event, an AI-focused extension of Microsoft's annual flagship developer event brand, Microsoft Build, took place on February 20, 2024 at the iconic Museum of the Future in Dubai, uniting government officials, technologists, innovators, IT decision-makers, and business professionals under one roof to share ideas and insights on the transformative power of Artificial Intelligence (AI) technologies.

"AI today is transforming every industry, and business leaders around the world are increasingly leveraging it to unlock new opportunities for growth, creativity and productivity," said Naim Yazbeck, General Manager, Microsoft

UAE. "We are proud to bring our flagship developer event, 'Microsoft Build: AI Day', to the UAE to empower business and IT professionals to keep pace with this rapidly advancing field. We look forward to engaging with the local developer community and providing a platform for them to expand their knowledge about the latest AI advancements, connect with various Microsoft experts, and elevate their skills to deliver more value faster across industries."

'Microsoft Build: AI Day' in Dubai featured keynote addresses, breakout sessions, and fireside chats by esteemed officials and experts including Dr Mohammed Al Kuwaiti, Head of the UAE's Cybersecurity Council; and Dr. Andrew Jackson, Chief Officer at IIAI, a G42 company. Various Microsoft executives including Julien Bertin, Azure Lead

for Microsoft CEMA; Hakki Ogretmen, Application Innovation Lead at Microsoft UAE; and Aysar Yousef, Azure Data & AI Lead, FSI & Aviation Industries, will also deep dive into topics such as integrating the power of cloud and AI into development workflows, and how to build and scale cloud-native, intelligent applications on Azure.

Microsoft experts will also highlight the latest advancements in Generative AI and how they are inspiring developers to create innovative AI applications such as virtual assistants, content generation, code generation, image editing tools, and more. Speakers will also showcase how developers can access the most advanced AI models including Dall-E 2, GPT-3.5, GPT-4, Codex, and ChatGPT using the Azure OpenAI Service. Special sessions will also be dedicated for building and maintaining Microsoft Copilot with Azure Machine Learning and GPT-4, and on using the latest AI models responsibly.

The event will also feature the AI Innovation Award that recognizes individuals and organisations that have demonstrated unparalleled excellence in driving digital transformation with AI. "Over the past year, we have witnessed innovators and businesses across various sectors leverage the latest developments in AI to deliver cutting-edge solutions that are tackling key industry challenges, driving digital transformation efforts, and creating a positive impact on society. It gives us great pleasure to celebrate the extraordinary achievements of this community, and we look forward to collaborating with them as they continue to push the boundaries of innovation and create the next generation of responsible and impactful AI solutions," said Mohamed Mikou, Chief Operations Officer and Chief Marketing Officer at Microsoft Central Europe, Middle East and Africa. 🌟





#GISEC | CYBER.GISEC.AE

THE SUPER CONNECTOR FOR THE MIDDLE EAST & AFRICA'S CYBER SECURITY COMMUNITY

SCAN ME



GISEC is the ideal cybersecurity platform to participate & partner with vendors and government entities in the region.

H.E. DR. MOHAMED AL-KUWAITI
Head of Cyber Security,
United Arab Emirates Government



ENQUIRE ABOUT EXHIBITING, SPONSORSHIP & SPEAKING OPPORTUNITIES: +971 (04) 308 6469 | GISEC@DWTC.COM

HOSTED BY



OFFICIAL GOVERNMENT CYBERSECURITY PARTNER



OFFICIALLY SUPPORTED BY



OFFICIAL DISTRIBUTION PARTNER



GOLD SPONSOR



ORGANISED BY



EXCLUSIVE FEATURE: DATA PRIVACY

IN AN ERA DOMINATED BY DIGITAL INTERACTIONS, DATA PRIVACY DAY, MARKED IN JANUARY EVERY YEAR SERVES AS A STARK REMINDER OF THE CRITICAL NEED TO SAFEGUARD CRITICAL INFORMATION. AS CYBER THREATS ESCALATE, THIS EXCLUSIVE FEATURE BY SECURITY ADVISOR MIDDLE EAST EXPLORES THE SIGNIFICANCE OF SECURING DATA IN OUR DAILY LIVES, WITH EXPERTS THROWING LIGHT ON THE PIVOTAL ROLE DATA PRIVACY PLAYS IN MAINTAINING ENTERPRISE AND PERSONAL SECURITY.

Spokespersons

Bernard Montel, EMEA Technical Director and Security Strategist, Tenable
Christopher Budd, Director Threat Research at Sophos
Dave Russell, VP of Enterprise Strategy at Veeam
Ezzeldin Hussein, Regional Director, Sales Engineering, META at SentinelOne
Dr. Johannes Ullrich, SANS fellow and Dean of Research at the SANS Technology Institute
Joseph Carson, Chief Security Scientist & Advisory CISO, Delinea
Mohammed Eissa, Regional Sales Director, MEA, Entrust
Morey Haber, Chief Security Officer, BeyondTrust
Ramzi Itani, Regional Director at Veritas Technologies
K S Sreedharan, Director of Compliance, ManageEngine, Zoho Corporation
Tim Wade, Deputy Chief Technology Officer, Vectra AI

Bernard Montel

EMEA Technical Director and Security Strategist, Tenable

Each year we talk about data privacy and each year the number of individuals who've had their data breached increases. While it's important that individuals have a right to data privacy, if hackers are able to steal it, read it, publish it then there is no privacy. The reality is you can't have privacy without safeguarding it.

Threat actors can aggregate leaked data from numerous breaches into a single large database that can then be cross-referenced to launch further attacks. As illustration, the identity and password combination from one service can be used to breach another, referred to as 'credential stuffing'; by combining high level information from different sources to completely profile an individual — such as passwords, PINs, social security number, place of birth, and more, they could have enough information to answer security questions used to protect and/or access bank accounts. The more data available to hackers, the greater the risk becomes.

We must address inadequate security to stop threat actors stealing data. We know threat actors' attack methodology is not advanced or even unique but opportunistic. They see many ways in and multiple paths through environments to do damage and monetise their nefarious efforts. The widespread adoption of cloud computing introduces new levels of vulnerability and management complexity that can be targeted by bad actors.



Christopher Budd

Director Threat Research at Sophos



1. Remember the power of "no".
2. Be smart about your passwords.

Remember the power of no: this means remembering that the best way to protect your data and information is to not give it away in the first place. Just because a site asks you for your birthday, for instance, doesn't mean they need it or they're entitled to it. If a site or service doesn't have your information, they can't lose it or accidentally disclose it. While this may seem obvious, it's important and we can all remember this, always.

Being smart about your passwords: this means that while we all hate passwords, we all know they're a pain, they remain important. Even today we see major companies compromised because of bad password management by them or their people. Using unique passwords for every site (or at least every important site) is still one of the best things you can do to keep yourself secure. In addition to unique passwords, using a multifactor authentication app like Google Authenticator or Microsoft Authenticator is an important step in making those critical accounts even more secure.

Dave Russell

VP of Enterprise Strategy at Veeam

Cyber threats like ransomware play a critical role in organisations' ability to keep their data safe. Knowing how public attacks have gotten and considering consumer demands for better transparency into business security measures, there's more awareness around ransomware in 2024. New research supports the idea that ransomware continues to be a 'when' not 'if' scenario, with 76 percent of organisations attacked at least once in the past year, and 26 percent attacked at least four times during that time. Data recovery should be a key focus around Data Privacy Day 2024, knowing that it's still a major concern as only 13 percent of organisations say they can successfully recover during a disaster recovery situation. In 2024, the overall mindfulness of cyber preparedness will take precedence.



Ezzeldin Hussein

Regional Director, Sales Engineering, META at SentinelOne



In an era dominated by digital connectivity, the significance of privacy has become paramount. As individuals navigate the sophisticated web of online interactions, it is crucial to recognise the profound impact that personal data can have on one's life. The exponential growth of technology and the ubiquity of data-driven services underscore the need for heightened awareness about privacy. Every click, search, and interaction generates a trail of personal information, creating a digital footprint that can be exploited if not handled responsibly. To safeguard against potential threats, individuals must embrace best data protection practices, understand the value of their personal information, and take proactive steps to secure it. This involves using robust passwords, enabling two-factor authentication, and staying informed about privacy settings across various online platforms.

By creating a culture of responsible data handling at all levels of society, we can collectively build a more secure and respectful digital landscape. It is imperative to recognise privacy not as a mere convenience but as a fundamental right that demands our vigilance and commitment to ethical data practices, ensuring a safer and more secure online environment for everyone.

Dr. Johannes Ullrich

SANS fellow and Dean of Research at the SANS Technology Institute



Data security faces numerous threats. Our Internet Storm Center and SANS Institute monitoring has revealed significant vulnerabilities and attack methods that jeopardise data security.

One such threat is the vulnerability in Ivanti's connect secure VPN solution, widely used to control personal data access. Recent severe vulnerabilities in this product have transformed it from a protective tool into a potential gateway for attackers, undermining organisational data controls.

Another prevalent threat is password spraying. A recent example includes a cyber-attack on Microsoft, leading to data exposure from its executives and cybersecurity team. Through our honeypot investigations, we have gathered data on the common passwords used in these attacks, which can assist organisations in strengthening their internal password policies to prevent brute force or spraying attacks.

Joseph Carson

Chief Security Scientist & Advisory CISO, Delinea

The end of privacy as we know it might be closer than you think. The world is increasingly relying on more AI and machine learning technologies. This reliance could result in privacy becoming less and less of an option for individuals, as AI's capabilities in surveillance and data processing become more sophisticated.

2023 marked a significant leap in the authenticity of deepfakes, blurring the lines between reality and digital fabrication, and that is not slowing down any time soon. Our digital identities, extending to digital versions of our DNA, can be replicated to create digital versions of ourselves, which can lead to questioning who actually owns the rights to our online personas.

Unfortunately, advancements in AI technologies are evolving more swiftly than current regulations can keep pace with. In 2024, we can expect stricter data protection requirements across more countries and regions. But until these regulations evolve and can keep pace, it is important to reduce our risk and protect our privacy however possible.



Mohammed Eissa,

Regional Sales Director, MEA, Entrust



This year, Data Privacy Day serves as a stark reminder that safeguarding digital identities must take center stage in our increasingly interconnected world. The so-called conflict between "seamless user experience" and security is over -- the only answer is that security has to be welcomed as part of the experience.

Over the past few years, data breaches and privacy scandals have become alarmingly commonplace, raising concerns about the security of our personal information. From large-scale corporate breaches to individual cases of identity theft, the threats to our digital privacy persist and continue to evolve.

As technology continues to advance at a rapid pace, so too do the tools and techniques employed by malicious actors. From sophisticated hacking attempts to more subtle forms of data mining, our personal information is constantly under siege. Even the most highly-trained security professionals may miss increasingly realistic AI-generated phishing scams, across text, voice, and video.

Governments and regulatory bodies across the Middle East continue strengthening the fight against an ever-evolving threat landscape. For instance, UAE's Dubai International Financial Centre (DIFC) recently announced modifications to its current data protection laws, perhaps of the most important of which are the newly included AI clauses.

Ramzi Itan

Regional Director at Veritas Technologies

Data Privacy Day serves as an important reminder for IT leaders in all organisations across the Middle East region of the scale of growing cyber threats to their data, as well as the business risks presented by non-compliance with the rapidly evolving regulatory landscape, designed to keep data safeguarded. In line with this year's theme of 'Taking Control of your Data,' the role of Artificial Intelligence, and its relationship to our data protection cannot be overlooked.

While the transformative impact of Artificial Intelligence (AI) on the way we manage our data is evident, AI's swift evolution has given rise to new challenges, notably seen in the surge of autonomous ransomware attacks.

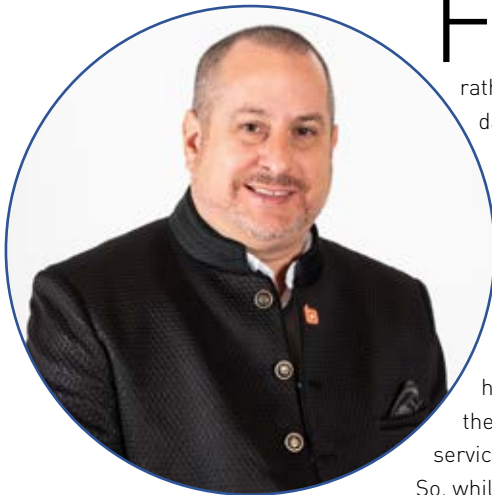
Veritas' Data Risk Management report revealed that 73% of UAE organisations fell victim to ransomware attacks in the last two years. AI not only enhances threat detection but also empowers cybercriminals to execute sophisticated attacks.

As the Middle East tightens its data protection frameworks in response to these challenges, it is clear that vigilance and adaptability are not merely optional but essential and are also recognised as critical by individuals. Veritas research on the use of generative AI technologies in professional environments showed that 44% of employees questioned in the UAE understood that using public generative AI tools did introduce greater risks of sensitive information being leaked.



Morey Haber

Chief Security Officer, BeyondTrust



For Data Privacy Day this year, let's explore the controversial topic of impact of age demographics on perceptions of data privacy. This is not a discussion on whether data privacy is important, nor that sensitive information needs to be protected, but rather based on age groups, social media, and the designator of being an "influencer," data privacy means very different things.

As a matter of fact, younger generations, that have embraced social media as a primary vehicle for income or popularity, have decided personal data privacy is less important than older generations that prefer to keep even their own birthdays private. The reasons are not completely obtuse since younger generations are generally fearless, lack experience, and have embraced the idea that personal information, and the transparency of data privacy, can lead to quick wealth, social status, and can have no repercussions if exposed. For older generations, data privacy has different implications, based on world geopolitics, distant relationships, and even the desire to protect family and assets acquired through years of hard work or public service.

So, while we can all agree data privacy is important, it does not mean the same thing to everyone and age can play a significant role in determining what an individual considers private or not.

K S Sreedharan

Director of Compliance, ManageEngine, Zoho Corporation

Safeguarding data is a priority for business as well as for individuals. With every new technology, the risk profile changes, and with it, fresh challenges arise. The widespread use of AI and ML technology has pushed the boundaries of the amount of personal data that can be collected and analysed. This has led to the possibility of algorithms learning the behavior of a person and making decisions that impact the individual's rights. Large-scale data collection increases the risk of surveillance. Therefore, regulators in various geographies have developed mandates for the responsible use of AI and ML technologies. It is in the best interest of businesses to follow these mandates, as compliance violations can not only result in penalties but also the loss of trust in customers.

Another risk is that of decisions made by AI and ML technologies based on models trained on specific types of data in the form of images, videos, text, and numbers that pertain to the model. Such data, though carefully curated for training purposes, will still likely carry inaccurate information. There should always be a process requiring a human to review the automated decisions made by technology so corrective actions can be taken if needed.

There have also been instances where employees using AI technologies to simplify tasks for their jobs have inadvertently leaked sensitive company information. Organisations should educate employees about these risks and build controls to avoid them. Furthermore, there should be controls on the use of this collected data so that the purpose for processing it does not violate the published mandate. The processing of this data should be beneficial in terms of improving productivity but should absolutely not infringe on an individual's rights.



Tim Wade

Deputy Chief Technology Officer, Vectra AI



Customers and consumers alike are sharing more data than ever with organisations. This comes at a time when enterprises are shifting more applications, workloads, and data to hybrid and multi-cloud environments, and threat detection and response has become increasingly siloed and complex. Together, this underscores the crucial responsibility organisations have in safeguarding sensitive information and serves as a poignant reminder of the challenges involved in maintaining data privacy.

We've seen steady improvement on the part of the end user towards keeping their personal information secure and private. They deploy multi-factor authentication solutions, only use secure networks or VPNs, and are much more selective about which information they share with organisations, but exposure incidents still happen. As we strive to make the world a safer and fairer place, companies have a responsibility to their customers, partners, and end users to implement the right practices that will ensure their privacy and data are protected. In the upcoming year, businesses will face heightened expectations to demonstrate their commitment to implementing comprehensive measures aimed at safeguarding data.

INNOVATING BEYOND SECURITY

ANITA JOSEPH CAUGHT UP WITH **WESLEY WANG**, DIRECTOR OF CHANNEL DEVELOPMENT & MARCOM AT HIKVISION MEA, TO LEARN ABOUT THE COMPANY'S INNOVATION-FIRST APPROACH AND ITS PLANS FOR THE REGION FOR 2024.

Hikvision has been a prominent participant at Intersec for several years. Can you share some insights into the significance of this event for Hikvision, and what specific products, solutions, or innovations did you showcase at Intersec 2024?

As the largest and the most prestigious security industry exhibition in the Middle East and Africa Regions, Intersec is an event where Hikvision mobilises significant resources to engage with our customers and partners. Every year at Intersec, we get to see the latest solutions in the security industry and learn about what's trending. And it also gives us a good opportunity to reconnect with existing clients, and network to drive new business growth and opportunities.

This year at Intersec 2024, we showcased our industry's intelligent solutions in vertical markets, such as traffic, building, education, and energy.

Customers can also experience the whole suite of products empowered by Hikvision's core technologies in multi-dimensional perception across the full spectrum of light, radio, and sound.

We also display a wide range of our advanced LED display models, providing an industry-leading viewing experience to customers and prospects.

We look forward to connecting with our industry leaders and exploring innovative technologies to push the boundaries of the security industry.

AT HIKVISION, WE ARE COMMITTED TO SERVING VARIOUS INDUSTRIES THROUGH OUR CUTTING-EDGE TECHNOLOGIES.

Hikvision has been at the forefront of integrating artificial intelligence into its security solutions. Can you provide insights into Hikvision's current AI strategies and how AI is shaping the future of security technology?

As we know, technology has been moving fast in recent years and AI technology is available everywhere. At Hikvision, we are committed to serving various industries through our cutting-edge technologies of machine perception, and AI, thus leading the future of AIoT.

Hikvision provides a broad range of security products, covering video security, access control, and alarm systems. We also provide integrated security solutions powered by AI technology to support end-users with new applications and possibilities for safety management and business intelligence, including in the transportation, retail, logistics, energy, and education industries. In addition, Hikvision is extending its business to smart homes, robotics, automotive



electronics, intelligent storage, fire security, infrared sensing, X-ray detection, and medical imaging to explore new channels for sustaining long-term development.

Sustainability is the buzzword today. How does Hikvision incorporate sustainability into its products and operations?

Hikvision is committed to integrating corporate social responsibility and sustainability development philosophy into our business, while also being driven by technological innovation.

We launched a STAR Program for

Social Good which aims to provide cutting-edge technologies that help non-profit organisations and projects explore innovative ways to benefit communities and protect our valuable nature and culture. We're digging into low-carbon thinking and green practices, and constantly strive to create technologies and products that don't just benefit our partners and end users, but also the planet.

As we look ahead to 2024, what strategic initiatives and plans does Hikvision have in place to continue its growth and innovation in the security

technology sector?

In 2024, Hikvision's new business and product strategy is 'Innovating Beyond Security'.

This new approach is about pushing the boundaries of the conventional security industry. Hikvision will achieve this with a new range of multi-dimensional AIoT products and technologies across the spectrums of light, radio, and sound. Other key focus areas for 2024 include machine learning, deep market insights, and a sustainable development philosophy. We hope all of these will help create a better world for communities, employees, and businesses. 📌

WHY MUST SECURITY PROFESSIONALS USE PACKET DATA?

EMAD FAHMY, SYSTEMS ENGINEERING
MANAGER, MIDDLE EAST, NETSCOUT



With trillions of dollars at stake and cyber resilience impacting a wide range of business concerns, such as business continuity, customer privacy, and the pace of innovation, it's

clear that current approaches to combat attacks are insufficient. An effective cybersecurity strategy goes beyond compliance and technology, emphasising collaboration across business functions and necessitating active engagement from the CXOs and senior leaders who

grasp the strategic risks and can drive transformative change. A McKinsey study in collaboration with the World Economic Forum indicates companies are grappling with cyber risk management, highlighting an ongoing battle for organisations to protect themselves from a range of cyber risks, making robust security measures essential in the face of heightened stakes.

In the cybersecurity domain, the crucial task of protecting digital landscapes from threats heavily relies on network traffic analysis. At the core of this analysis is a valuable resource known as packet data. This term refers to information transmitted over a network, divided into small units called network packets, which include essential elements such as headers (containing source and destination addresses) and payload (the actual information being sent). This intricate network of packets holds significant importance for security experts, providing indispensable insights for strengthening defences and preventing malicious activities.

In the dynamic field of cybersecurity, analysing packet data provides security professionals with a vital advantage, offering granular insights, forensic capabilities, and detailed analysis essential for fortifying defences and safeguarding digital environments against evolving threats. Mastering the use of packet data is not just a choice;

it's a necessity for modern cybersecurity practitioners.

Here's why an individual should leverage packet data:

- **Threat detection and analysis:** Packet data plays a crucial role in both identifying anomalies and employing signature-based detection in the analysis of network traffic. Security experts can examine individual packets to identify unusual patterns, unexpected traffic, or deviations from normal behaviour, effectively pinpointing potential security threats. Furthermore, through the scrutiny of packet payloads, it supports the creation and deployment of signatures for recognised threats, assisting in the identification of specific attack patterns or malicious content within the network traffic.
- **Incident response and forensics:** Packet data plays a vital role in incident response by facilitating thorough forensic analysis and reconstructing network traffic. Security experts can reconstruct the events that led to security incidents or breaches, gaining insights into the nature, scope, impact, and the attack methods employed by threat actors. A detailed examination of packet data allows the reconstruction of the sequence of events preceding an incident, offering valuable understanding and context for effective incident response and mitigation efforts.
- **Network monitoring and performance analysis:** The analysis of packet data serves a twofold function, involving real-time monitoring and performance optimisation in network

environments. Network and security experts use packet data to assess current network traffic in real-time, detecting indications of intrusion, unusual activities, or performance decline. Furthermore, through the examination of packet data, they identify network bottlenecks, latency problems, and errors, allowing for the implementation of effective optimization strategies to improve overall network performance.

- **Security tool enhancement:** Integrating packet data with security tools like intrusion detection systems (IDSs), intrusion prevention systems (IPSs), or security information and event management (SIEM) systems strengthens their capabilities and accuracy in detecting threats. The incorporation of packet data improves the performance of these security solutions, allowing for more precise and effective identification of potential threats in network environments.
- **Protocol analysis and vulnerability identification:** Packet Data analysis provides a thorough approach by enabling the examination of network protocols for vulnerabilities, misconfigurations, and potential points of exploitation. Moreover, it supports the inspection of payloads within packets, identifying malware, exploits, or unauthorised attempts at data exfiltration. This dual capability empowers security experts to delve deeply into both vulnerabilities at the protocol level and specific content within packet payloads, ensuring comprehensive security assessments.

Neglecting to carefully employ specific

use cases reliant on packet data can lead to severe consequences for both security professionals and an organisation's cybersecurity infrastructure. This encompasses the danger of undetected malware and security threats, unattended protocol vulnerabilities, restricted incident response and forensic capabilities, heightened exposure to security risks, diminished efficacy in security operations, and inadequate compliance and reporting. The absence of packet payload scrutiny introduces risks such as persistent malware activities, potential vulnerability exploitation, difficulties in reconstructing events during incidents, heightened vulnerability to security risks, inefficiencies in addressing emerging threats, and the possibility of compliance and legal consequences due to incomplete reporting.

NETSCOUT provides tools for security professionals, offering insights into network traffic through packet data capture capabilities. The platform excels in threat analytics, recognising known indicators, vulnerable protocols, and unusual behaviour. With sophisticated packet analysis tools, NETSCOUT enables professionals to examine payloads, scrutinise protocols, and reconstruct events during investigations, equipping them to strengthen defences and respond to evolving cybersecurity challenges with confidence.

All in all, the utilisation of packet data emerges as a pivotal strategy for security professionals navigating the complex landscape of cybersecurity. Its importance is underscored by the potential risks associated with its neglect, emphasising the critical need for organisations and professionals to integrate packet data into their cybersecurity frameworks. As cyber threats continue to evolve in sophistication and frequency, harnessing the power of packet data becomes indispensable, ensuring robust defence mechanisms, effective incident response, and proactive identification of vulnerabilities. 🛡️

ANALYSING PACKET DATA PROVIDES SECURITY PROFESSIONALS WITH A VITAL ADVANTAGE, OFFERING GRANULAR INSIGHTS, FORENSIC CAPABILITIES, AND DETAILED ANALYSIS.

BEYONDTRUST CONTINUES TO DELIVER INNOVATION AND PROFITABLE GROWTH IN 2023

BeyondTrust, the leader in intelligent identity and access security, has announced significant recurring growth in

2023 and continued innovation through expansion of its identity security platform, acquisition of new customers, and delivery of exceptional customer and employee experiences.

Key 2023 highlights include:

- Accelerating recurring revenue to greater than 80% of total revenue, with approximately 40% YoY subscription ARR growth
- Driving substantial new business, adding nearly 1,500 new logos
- Expanding current solutions for about 3,700 current customers with new products or add-ons
- Achieving gross retention of more than 95% and net retention rate of more than 110% for implied renewals, along with an industry-leading Net Promoter Score (NPS) of 62 and Customer Satisfaction (CSAT) score of more than 95%
- Delivered profitable growth with Adjusted EBITDA (GAAP) in excess of 25%, exceeding the "Rule of 40"

To drive growth and continued



innovation in the identity security market, BeyondTrust has added two new members to the Executive Leadership Team:

- Brett Theiss joined BeyondTrust as Chief Marketing Officer
- Sean Cashin was appointed Chief Customer Officer

Demonstrating continuing innovation leadership, BeyondTrust released advanced capabilities across the BeyondTrust Platform in 2023 to provide customers with unmatched visibility and control in their relentless battle against sophisticated cyber threats. The launch of Identity Security Insights delivers industry-leading visibility, threat detection, and proactive security recommendations across the entire identity estate. Identity Security Insights consolidates the capabilities of PAM, CIEM, and ITDR, providing organisations with a robust toolset to preempt and neutralise identity-driven threats, exemplified by the recent discovery of the Okta Support breach.

Additional capabilities introduced in the past year include:

- **Privilege Management for Windows and Mac:** A new level of automation has been added to revolutionise the upgrade process, with a new auto update feature that helps customers drastically reduce the amount of manual work required from their IT and security teams.
- **Password Safe:** The introduction of a new Web Portal provides customers with a more intuitive, streamlined, and productive user experience to improve performance and accessibility.
- **Workforce Passwords:** This new add-on capability for Password Safe helps customers manage business application user passwords and non-SSO applications without additional complexity and with the enterprise-level security.

- **Privileged Remote Access:** The introduction of Cloud Infrastructure Access functionality, including ephemeral Jump clients, enables developers, cloud ops engineers, and technical workers to securely and more easily access critical cloud platforms, applications, and data.
- **Remote Support:** Real-time chat translation is now available via an integration with AWS Translation Services, enabling reps to provide localized support chat to their customers in over 75 languages in real time, without a language barrier.
- **Privilege Management for Unix/Linux & Active Directory Bridge:** The introduction of support for cached policies and logging enables organizations with Linux workstation deployments to keep users productive and estates secure, regardless of the presence of unreliable connectivity.

In addition to significant product releases, BeyondTrust demonstrated its ongoing commitment to serving the evolving needs of its customers with several security-focused initiatives:

- **ISO 27001:2022 Re-certification:** Alignment with the new ISO 27001:2022 control establishes a

structured approach to managing and preserving sensitive information and serves as a testament to BeyondTrust's all-encompassing Information Security Management System (ISMS), covering the development, operation, and administration of its products.

- **Participation in the Amazon Web Services (AWS) Independent Software Vendor (ISV) Workload Migration Program (WMP):** Customers benefit from a streamlined transition to the cloud that upholds robust security and compliance standards.
- **Enhancement of the PartnerTrust:** Deeper partner engagement facilitates more successful customer outcomes in a collaborative partner ecosystem.
- **FedRAMP Moderate "In-Process" Status:** FedRAMP authorisation will increase BeyondTrust's capacity to serve federal agencies and deliver secure cloud deployment and achieving "In-Process" status has already helped the company to achieve record growth in the public sector in 2023.
- **BeyondTrust and Carahsoft Grants Support Program:** Public sector agencies, educational institutions, and tribal communities benefit from grants information, customised funded research, and consultation as they develop project ideas, get technology-rich projects funded, and expand initiatives.

"We achieved significant momentum in 2023, driven by robust revenue growth, product expansion, and industry and partner recognition," said Janine Seebeck, CEO, BeyondTrust. "I take great pride in our employees and partner ecosystem for their dedicated efforts in service of our customers, and I am excited for the year ahead as we continue to help our customers solve their identity security challenges." 📌

**BEYONDTRUST
RELEASED ADVANCED
CAPABILITIES ACROSS
THE BEYONDTRUST
PLATFORM IN 2023 TO
PROVIDE CUSTOMERS
WITH UNMATCHED
VISIBILITY AND
CONTROL.**



AT THE FOREFRONT OF DIGITAL TRANSFORMATION

ANITA JOSEPH CAUGHT UP WITH **GUSTAVO GASSMAN** - VICE PRESIDENT, EMERGING MARKETS, AT HID, TO DISCOVER HOW THE COMPANY IS USING SECURITY AND TECHNOLOGY TO ENHANCE USER EXPERIENCE.

What is the outlook for HID in 2024?

HID's outlook for 2024 is highly optimistic, building on our exceptional performance in 2023, particularly in emerging markets. We have a robust pipeline for the year and strong expectations from both our business and investment sectors. This will increase resource allocation, especially in the Middle East, where we'll see significant investments and expanded on-ground operations.

What trends does the access control sector anticipate worldwide versus GCC?

Some trends have been stable in the last few years and will continue. One of them that is important for HID is mobile. So having everything on the mobile phone is important as everyone uses it. So, mobile access is the same. As a result, we are investing many resources and solutions to give people the freedom to perform access control on mobile. So mobile is our latest trend acquiring popularity we see and where we are putting our efforts to improvise and work efficiently.

How are the global movements of digitalisation and sustainability impacting HID?

Digitalisation and sustainability are major driving forces for HID, and we're heavily invested in aligning with these trends. Mobile access is a prime example. By virtualising credentials, we eliminate plastic waste from traditional cards and reduce shipping needs, minimising our environmental footprint. This also aligns with the growing consumer preference for convenience and security offered by mobile solutions. Furthermore, we launched sustainable physical credentials made from bamboo, catering to workplaces and applications where personal devices are restricted. This innovative option further reduces plastic consumption and provides a responsible alternative for environmentally conscious customers. Our commitment to sustainability extends beyond product development. We optimise our logistics and internal processes to minimize resource usage and emissions. The combination of innovative products, strategic operations, and environmental awareness positions HID as a leader in the access control industry for the digital and sustainable future.

Can you tell us about your partnership with Apple for its wallet?

Absolutely! Our partnership with Apple Wallet unlocks seamless access experiences for users worldwide. Currently, we're live in 34 countries, and global coverage is on the horizon. While Apple determines the specific rollout timeline, we're thrilled with the positive response we've seen so far.

Here's what users can expect:

- Imagine ditching bulky keycards and storing your credentials on your iPhone or Apple Watch. Apple Wallet makes access effortless, whether entering an office, gym, or hotel room.
- Apple's robust security protocols always protect your credentials. With multi-factor authentication and biometric verification, unauthorised access is virtually eliminated.
- Apple Wallet seamlessly integrates with existing HID access control systems, making the transition smooth and user-friendly.

We're confident that Apple Wallet will revolutionize how people access physical



spaces. We're actively working with Apple to expand our reach and bring this innovative solution to the Middle East and beyond. Stay tuned for exciting updates!

How about the smart building systems changing the way the Access Control works?

Smart building systems transform access control from a simple security measure into a dynamic contributor to building intelligence. Beyond controlling who enters and exits, access control acts as a data powerhouse, feeding valuable insights to optimise smart building functions. By tracking occupancy through access control data, systems can adjust lighting, heating, and ventilation based on real-time needs, minimising energy waste and reducing operational costs. Additionally, integrated access control systems provide granular control over access rights, allowing for dynamic perimeter security adjustments and immediate responses to security threats. For example, specific doors can be automatically unlocked in an emergency for safe evacuation.

Building systems can learn individual preferences through access control data, such as preferred temperature settings or lighting levels. This data can personalise the occupant experience, boosting comfort and overall satisfaction. This can also be combined with other sensor information to gain deeper insights into building usage patterns and occupant behavior, thereby enabling data-driven decision-making for improved resource allocation, space optimisation, and predictive maintenance. HID is at the forefront of this integration, developing innovative solutions that harness the power of access control data to make smarter, more efficient buildings. The future of access control lies in its seamless integration with intelligent



systems, creating a truly connected and responsive built environment.

How have Hybrid Work Models impacted your business?

The rise of hybrid work models has been a boon for HID, accelerating the adoption of our mobile access solutions in a way we couldn't have predicted. We've been at the forefront of mobile access technology for over a decade. We saw its potential to streamline access control and offer unparalleled convenience, even before the pandemic's remote work surge. Flexibility became paramount with hybrid models blurring the lines between office and home. Employees needed seamless access remotely or in the office for a few days. This is where mobile access shines, offering secure and convenient entry via smartphones or wearables.

While some building owners worry

about reduced space utilisation due to hybrid models, we see a different opportunity. Mobile access offers valuable data insights on building usage patterns, allowing for optimised space allocation and resource management. This can lead to cost savings and even the creation of flexible co-working spaces.

Additionally, combining robust security with exceptional user experience is a rare feat. Mobile access achieves both. It eliminates physical keycards, reducing the risk of loss or theft and offering enhanced security by offering multi-factor authentication and biometric verification. Additionally, it eliminates the need for physical badge pickups and access control desk interactions, saving valuable time and effort for both employees and building managers.

The hybrid work trend is here to stay, and mobile access is perfectly positioned to evolve alongside it. We're constantly innovating and exploring features like secure guest access, visitor management, and integration with smart home systems. Mobile access will be key in shaping the future of secure and convenient workspaces. 🚀

DIGITALISATION AND SUSTAINABILITY ARE MAJOR DRIVING FORCES FOR HID, AND WE'RE HEAVILY INVESTED IN ALIGNING WITH THESE TRENDS.



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

Cybersecurity, everywhere you need it

www.fortinet.com

Copyright ©2023 Fortinet, Inc. All Rights Reserved.

FORTINET®

THE EVOLUTION OF ZERO TRUST

■ **DAVE RUSSELL**, VICE PRESIDENT, ENTERPRISE STRATEGY AT VEEAM

Around 18 months ago, I was writing about the “endless journey” to Zero Trust. I used the word “endless” because Zero Trust is a mindset rather than a product or a destination – it’s a target to aim towards. Like many things in cyber, it’s a matter of constant evolution. You have to adapt to survive and thrive in your environment. Even the idea of Zero Trust has had to evolve with the times.

Changing with the times

A cat and mouse game, an arms race – call it what you want – security has always been about adapting and evolving to stay ahead of threats. Bad actors constantly experiment and move the needle to get ahead of their targets. This is exactly what has driven so much innovation across the industry since the first-ever cyber-attack took place. It almost goes without saying that the security tools considered the benchmark when I started my career 35 years ago would be a paper shield against a modern cyber gang. It’s not just the tools that have had to evolve, but also the mindset – how we think about security and use the tools at our disposal has had to change.

Zero Trust is a prime example of this. Once, security was just around the perimeter, it was a moat around the

castle, but once you were in, you were in. As more and more enterprises worldwide have adopted Zero Trust as best practice, this has shifted. Security measures now need to be inside and outside – doors are locked, proof of identity is required, and people aren’t allowed access to parts of the castle if they don’t need to be there.

But the thing about evolution is that it never really stops.

Introducing Zero Trust Data Resilience

Even the most broadly used Zero Trust models have a few fatal flaws in the modern environment. Namely, they lack any kind of guidance in pivotal areas like data backup and recovery. This gap is significant as recent attacks often attempt to target backup repositories. For example, according to the Veeam Ransomware Trends 2023 Report, ransomware attacks targeted backup repositories in at least 93% of attacks in 2022.

Data backup and recovery systems are critical parts of enterprise IT and must be considered as part of the security picture. They have read access to everything, they can write data into the production environment and contain full copies of the business’s mission-critical data. Simply put, following modern Zero Trust principles to the letter makes you fairly water-tight when it comes to ‘traditional’ security, but leaves a huge gap in the

armour regarding backup and recovery.

But this is where we are. Zero Trust has become too limited in scope as threats have evolved, which is why the concept of ‘Zero Trust Data Resilience’ has been born. An evolution of Zero Trust, which essentially broadens the scope to ensure backup and recovery follow the same principles.

Bringing backup and recovery into the fold

The core concepts are the same. The principle of least privilege and assume breach mentality are still key. For example, backup management systems must be isolated on the network so that no unauthenticated users can access it. Likewise, the backup storage system itself must be isolated. Immutability is also key. Having backup data that cannot be changed or tampered with means if repositories are reached by attacks like ransomware, they cannot be affected by its malware.

Assuming a breach also means businesses shouldn’t implicitly ‘trust’ their backups after an attack. Having processes to properly validate the backup or ‘clean’ it before attempting system recovery is vital to ensure you aren’t simply restoring a still-compromised environment. The final layer of distrust is to have multiple copies of your backups – fail-safes in case one (or more) are compromised. The best practice is to

have three copies of your backup, two stored on different media types, one stored onsite, and one kept offline. With these layers of resilience, you can start to consider your backup as Zero Trust.

Taking the first steps

With Zero Trust Data Resilience, just like Zero Trust, it's a journey. You can't implement it all at once. Instead, follow a maturity model where you gradually implement new practices and refine and evolve these over time. For example, if you don't currently validate your backup data, start doing so manually and over time implement technology to automate and schedule routine validation processes.

The other key thing you need is buy-in - everyone in the organisation must be on the journey together. Senior leadership is key to implementing any broad changes across an organisation, but so is educating across the business on new processes and their need. Finally, for Zero Trust Data Resilience especially, the security and wider IT operations teams must be aligned. Backup often falls under the responsibility of the latter, but as this becomes more and more crucial for security posture, the two need to work together to prevent security siloes or gaps.

The journey to Zero Trust is endless. So much so that the exact destination evolves over time. My advice to businesses is that while Rome wasn't built in a day, it is better to start taking steps today, no matter how small, instead of postponing and being left behind. 📌



RESHAPING SECURITY

ANITA JOSEPH CAUGHT UP WITH **MARTIN GREN**, CO-FOUNDER OF AXIS COMMUNICATIONS, TO DISCOVER MORE ABOUT THE CUTTING-EDGE TECHNOLOGY AND SOLUTIONS OFFERED BY THE COMPANY AND THEIR INNOVATIONS FOR A SMARTER, SAFER WORLD.



What did you showcase at the recently concluded Intersec? Axis is proud to have announced

three new cutting-edge products which were on display at our stand, including AXIS Q1961-XTE, the world's first thermometric explosion-protection camera specifically designed and certified by Axis for Zone and Division 2 hazardous areas; AXIS D2210-VE, a high-frequency radar that can accurately detect, classify and track humans and vehicles; as well as AXIS XC1311, the first network horn speaker from Axis certified for Zone and Division 1 hazardous areas.

Beyond this, we showcased the latest advancements in security technology under the theme 'Innovating for a smarter safer world.' Our booth featured interactive elements where visitors could engage with solutions through touchscreen displays and augmented reality. Visitors also had the opportunity to dive into the future of urban living as well as participate in our TCO game, an interactive experience that reveals the



extensive value and efficiency of Axis solutions.

Tell us about your World First that you displayed

AXIS Q1961-XTE Thermometric Camera represents a groundbreaking innovation as the world's first explosion-protected thermal camera specifically designed and certified for use in Zone and Division 2 hazardous areas, areas containing potentially combustible substances. These hazardous areas, notably larger than Zone and Division 1 areas, constitute the majority of hazardous area sites.

With the capacity to remotely monitor temperatures ranging from -40°C to 350°C (-40°F to 660°F), this economically efficient camera excels in monitoring temperature-related events. It sends notifications to operators based on temperature readings and fluctuations, thereby significantly mitigating the risk of production downtime and facilitating predictive maintenance planning.

Anticipated for release through Axis distribution channels in March 2024, AXIS Q1961-XTE stands as a pivotal tool in enhancing operational safety and efficiency in hazardous environments.

How is the security industry set to make an impact for enterprises this year?

The security industry is expected to make a significant impact on enterprises in 2024 by leveraging advanced technologies such as artificial intelligence (AI) and machine learning (ML) used for analytics. These technologies will enable more proactive and intelligent security measures, allowing enterprises to better anticipate and prevent threats. But it will also enable enterprises to be more operationally efficient, and to make smarter decisions – offering value beyond security.

Additionally, the integration of cybersecurity and physical security will become increasingly important in creating a comprehensive security framework for enterprises. This convergence will help

organisations effectively manage and mitigate security risks across their digital and physical assets.

What is Axis role in leading the UAE to becoming a global capital for surveillance industry?

The development and growth of the surveillance industry in any country involves a combination of factors such as government initiatives, technological advancements, regulatory frameworks, and the efforts of various companies within the industry. Axis' role in growing the UAE's surveillance sector is through providing advanced surveillance technology, collaborating with local authorities, and participating in projects related to security and surveillance infrastructure.

What are your plans for Axis in 2024?

Here in the Gulf region we are seeing very good growth and are expanding our operations in many of our locations. As an example, we are extending the Riyadh office with plans for building a new Experience Center where we can showcase our products and solutions. Locally in Dubai we will also continue to update our local customer experience center and ensure that our clients are exposed to industry trends, latest innovations and best-in-class products. 📌

THE INTEGRATION OF CYBERSECURITY AND PHYSICAL SECURITY WILL BECOME INCREASINGLY IMPORTANT IN CREATING A COMPREHENSIVE SECURITY FRAMEWORK FOR ENTERPRISES.

WHY ENERGY AND UTILITY SECTORS CONTINUE TO BE TARGETED BY THREAT ACTORS

MERIAM EL OUAZZANI, REGIONAL DIRECTOR - MIDDLE EAST, TURKEY, AFRICA AT SENTINELONE

On May 7, 2021, a ransom note was uncovered by a Colonial Pipeline employee, revealing a successful systems breach attributed to the DarkSide ransomware group. DarkSide had managed to exploit an outdated virtual private network account, the first step leading to one of the most significant cyberattacks on the energy infrastructure in US history.

At the onset of the invasion of Ukraine in early 2022, Ukrainian government officials revealed that state-sponsored threat actors aimed to compromise the Ukrainian power grid, intending to trigger a blackout that would have impacted a staggering 2 million people.

The energy sector powers all other industrial, business, consumer and services sectors, and is the centre of all critical infrastructure. The attack surface of the energy sector exists at every point on the power chain. This dependency on widely dispersed networks and industrial control systems creates vulnerabilities that threat actors find attractive.

Lucrative Returns

In May 2021, Colonial Pipeline's CEO paid a ransom of \$4.4 million dollar considering the essential nature of the company's infrastructure. Threat actors continue to target the energy and utilities sector because of the high probability of hefty ransom payments from enterprises in this sector.

Increasing Attack Surface

Rapid digital transformation within the energy and utilities sector is expanding its attack surface. Digital platform integrations, cloud adoption, Internet of Things have introduced many additional points of entry for threat actors. The energy sector also has widespread interconnections with many sub-systems.

Third-party Suppliers

By nature of their business, the energy and utilities ecosystem always has a large number of dispersed assets. This is a logistical and technological challenge for the enterprise's security administrators. The energy and utilities ecosystem is a blend of public and private strategic partnerships and involves third-party suppliers as well. Each of these components needs to be responsible for its own protection as well. However, the energy and utility entity also bears the responsibility of overseeing the security of the third-party ecosystem to ensure comprehensive end-to-end security coverage.

Connectivity Between OT and IT Systems

Large-scale industrial systems continue to be managed through SCADA process control systems also referred to as operational technology systems. These industrial systems manage energy production, energy distribution, and energy transmission. These control systems are now increasingly interconnected with information technology systems to improve data interoperability. This interconnection is

helping the movement of data but is also increasing vulnerability to threat attacks.

Here are some recommended best practices for protection against nation threat actors in the energy sector using industrial and information technology networks.

Strengthen Supplier Relationships

All data exchanges between suppliers should be via software applications and a software bill of materials. Enterprises should implement a shared cyber security responsibility with their suppliers. This will increase the level of performance required during the procurement process but will help to understand and improve the risk profile of suppliers.

Hardware Authentication

Geographically dispersed operational technology networks in the energy sector can be secured through hardware-based user authentication. This best practice requires the use of a dedicated physical device, typically a token or hardware key, alongside a primary user authentication password. Hardware authentication ensures that only authorized personnel with the correct physical device can enter the designated network.

User Behaviour Analytics

User-behaviour analytics builds predictable models of user behaviour around established work patterns of user behaviour. The strength of user behaviour analytics lies in its ability to raise alerts around unusual or suspicious network activities based on an understanding of a typical user's interactions with a particular environment.



Deep Network Visibility

Deep system and network visibility, coupled with real-time monitoring, detection, and response capabilities, are security essentials for the energy sector. Advanced security solutions such as autonomous and AI-powered XDR can offer a comprehensive view of both information technology and operational technology environments.

This proactive approach is critical in safeguarding critical energy infrastructure against cyber threats that could disrupt operations. Enterprises should look for a cybersecurity vendor who can provide these measures of protection and management. 📌

THE ENERGY SECTOR POWERS ALL OTHER INDUSTRIAL, BUSINESS, CONSUMER AND SERVICES SECTORS, AND IS THE CENTRE OF ALL CRITICAL INFRASTRUCTURE.

SANS INSTITUTE INTRODUCES PIONEERING COURSE ON AI LEADERSHIP

In an era where artificial intelligence (AI) is transforming every facet of business, the SANS Institute, a global leader in cybersecurity training, is proud to announce the launch of a pioneering new course: AIS247: AI Security Essentials for Business Leaders. Tailored specifically for the manager level and above, this cutting-edge 90-minute online course, led by renowned expert and SANS Fellow Frank Kim and SANS Head of Innovation and course author Dan deBeaubien, is designed to empower leaders with the knowledge and tools needed to navigate the complexities and opportunities of AI in the business world.

AI is no longer a futuristic concept but a present-day reality reshaping industries across the globe. With the rapid evolution of Generative AI (GenAI) technologies, understanding their strategic implications, operational mechanics, and associated risks is crucial for business leaders. AIS247 addresses this critical need, offering comprehensive insights into AI adoption, tools, operations, and the pivotal role of cybersecurity in AI development.

Participants will benefit from an in-depth exploration of GenAI and understand its foundations, including prompt engineering and large language models. The course takes a hands-on approach, with practical applications to showcase how GenAI is revolutionising industries through examples in content creation, data analysis, software engineering, and more.

One of the course's focal points is risk management and mitigation, providing crucial insights into common GenAI risks. Participants will not only identify potential threats but also acquire effective strategies for risk mitigation, ensuring a proactive and resilient



security posture. Additionally, AIS247 addresses the critical aspect of AI policy development, equipping participants with the skills needed to craft and implement effective AI strategies within their organisations. This comprehensive approach ensures that business leaders are not only informed about GenAI but are also prepared to navigate its risks and opportunities strategically, creating a secure and forward-thinking organisational AI framework.

"This course is an essential guide for any professional striving to stay ahead in a world increasingly driven by AI," Kim said. "The course provides invaluable takeaways and skills, including

understanding the motivations for GenAI adoption, addressing primary risks in AI implementation, and appreciating the ethical considerations in AI usage."

Enrollment is now open, with a single-seat price of \$289 and volume discounting available. This training is a rare opportunity to gain a competitive edge in the realm of AI - a field where staying informed is not just beneficial, but imperative for success.

Register now for AIS247: AI Security Essentials for Business Leaders and embrace the AI evolution with confidence and competence: <https://www.sans.org/cyber-security-courses/ai-security-essentials-business-leaders/> 🔑

DAP-2622



Wall-Plated Access Point

*Convert any Ethernet socket
into a high-speed Wi-Fi hotspot*

The DAP-2622 is equipped with two PoE ports, which are able to power an external device (such as an IP phone), as well as a LAN port if a wired connection is necessary.

Nuclias Connect AC1200 Wave 2 Wall-Plate Access Point



x3 LAN ports

Three LAN ports offer the option to expand your wired network, including the option to connect and power an additional PoE device, such as a VoIP phone.

- * Minimise the hassle of admin tasks
- * Flexible installation with PoE
- * Multiple Operation Modes
- * Super-fast Wireless AC Performance

Easy to manage
with D-Link's FREE
software-based
management solution



Nuclias Connect





BAHWAN
CYBERTEK

ACCELERATE YOUR DIGITAL TRANSFORMATION TO UNLOCK BUSINESS VALUE

YOU CAN COUNT ON US

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

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

1000+
Customers

20+
Countries

4000+
Associates

20+
Partnerships

USA | Singapore | Malaysia | Brunei | Taiwan | India | Oman | UAE | Qatar | Saudi Arabia

www.bahwancybertek.com