ISSUE 78 | OCTOBER 2023

Se

WWW.TAHAWULTECH.COM

ADVISOR

MIDDLE EAST

CYBER IMMUNITY IS THE FUTURE OF CYBERSECURITY

RASHED AL MOMANI, GENERAL MANAGER OF MIDDLE EAST AT KASPERSKY, TELLS ANITA JOSEPH HOW THE COMPANY IS LEADING INNOVATION IN CYBER IMMUNITY AND HELPING GOVERNMENTS TO STAY ONE STEP AHEAD OF THREAT ACTORS WITH THREAT INTELLIGENCE.

🛞 tahawultech.com







Innovative Solutions for a New Era of Security, Resilience & Productivity

Join us at **HALL 3**



info@starlinkme.net | www.starlinkme.net

WITH LIMITLESS OPPORTUNITIES

Spark Your

Growth

CONTENTS







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

CYBER IMMUNITY

IS THE FUTURE OF CYBERSECURITY

16 Bernard Montel, EMEA Technical Director and Security Strategist at Tenable, on how Al is reshaping the threat-security landscape and how Tenable is driving this change. **47** Special Report on how LinkShadow is reshaping the cybersecurity landscape with its innovative, cutting-edge solutions.

60 Abdullah ALSaadoun, Director META, at NetWitness, on the company's comprehensive, end-to-end visibility equipped with diverse security capabilities.



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.



EDITOR'S NOTE



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

> Anita Joseph Editor

EVENTS



REWRITING THE FUTURE

TECHNOLOGY IS

CO-AUTHORING OUR

FUTURE

n the grand narrative of human progress, there exists a remarkable recurring theme – the profound impact of technology on our future. With every breakthrough, from the invention of the wheel to the advent of artificial intelligence, we find ourselves at a new chapter in our story, one that is being written by the very tools we create. Today, as we navigate the digital age, it's abundantly clear that technology is not just a supporting character; it has become the author of our future.

The pace at which technology is rewriting the future is nothing short of astounding. Consider

the smartphone in your pocket, a device that not only connects you to the world but also serves as a personal assistant, navigator, and storyteller of your life. Or think about the remarkable strides in healthcare, where precision medicine and telemedicine are transforming how we diagnose and treat illnesses, offering a glimpse into a future where diseases are conquered more swiftly and effectively. To underscore this fact, GITEX 2023, the world's largest technology show, will shine the spotlight on how new and emerging technologies, particularly AI, is transforming the way we live, work and think.

The journey into the future is not without its challenges and ethical dilemmas. Questions about data privacy, job displacement, and the responsible use of powerful technologies loom large. But

> these questions also highlight the importance of our role as co-authors of the future. We have the power to shape the

narratives that technology unfolds, but the question that remains is: What story will we collectively author with the powerful tools at our disposal? It's a question that demands our attention, care, and responsibility as we journey forward into the next chapter of our future, guided by the ever-mighty hand of technology.

Published by

Dominic De Sousa (1959-2015)

FOUNDER, 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 Snehajan webmaster@cpimediagroup.com Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai. UAF

Tel: +971 4 5682993

© Copyright 2023 CPI All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

ar Syed imediagroup.com a

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

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

Online Editor

Contributing Editor SAME & Tahawultech Veronica Martin _____

NEW ZERO TRUST SOLUTIONS FROM ENTRUST ENHANCE SECURITY OF APPLICATIONS, ENCRYPTION KEYS AND SECRETS



Entrust, a global leader in identity

and data security, has announced new capabilities to help organisations enhance their security posture and advance their Zero Trust maturity journey. The new features extend protections, visibility, and governance over virtual infrastructures, code and application development, and cryptographic key management.

"IT and security leaders are being challenged to secure the enterprise. anticipate, and plan for new threats, ensure compliance, and enable the organisation to advance and grow. Zero Trust offers a framework for organisations to enhance their security posture, while enabling today's hybrid, multi-cloud operations. These latest innovations from Entrust help organisations gain greater visibility and governance over how they manage encryption keys, secrets, and applications across on-premise, virtualised and multi-cloud operations," said Bhagwat Swaroop, President, Digital Security Solutions at Entrust.

Entrust has created a new Zero Trust Maturity self-assessment to help organisations understand how their posture aligns with the CISA Zero Trust Maturity model. Read below for more details on how each of these innovations help organisations enhance their Zero Trust frameworks.

TENABLE RECOGNISED AS A LEADER IN OT SECURITY IN LATEST GIGAOM RADAR REPORT

Tenable, the Exposure Management

company, has announced it has been named a 'Leader' in the GigaOm Radar for Operational Technology (OT) Security. GigaOm Radar reports provide forwardlooking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution.

GigaOm Analyst Chris Ray said: "Tenable OT Security is comprehensive, provides numerous mature integrations, supports complete ICS/OT protocol decoding, delivers high-quality alerts, and leverages vulnerability priority ratings (VPR) to significantly reduce the time it takes to remediate or mitigate risk. Tenable uses a proactive approach to exposure management by limiting the attacker's ability to exploit vulnerabilities, preventing them from becoming active threats."



"GigaOm's recognition further validates Tenable OT Security's market leadership and product strategy as a unified solution purpose-built to secure OT, IT, and IoT devices in operational environments," said Amir Hirsh, General Manager, OT Security at Tenable. "As leaders in exposure management, Tenable has earned the trust of customers and industry experts across the globe, including OT and industrial cybersecurity professionals, and we are thrilled to add GigaOm's recognition as a leader in their Radar for OT Security report to this growing list."

COMMVAULT CONTINUES TO LEAD IN GIGAOM RADAR REPORT: HYBRID CLOUD DATA PROTECTION FOR LARGE ENTERPRISES

Commvault, an enterprise data

protection leader for today's global businesses, has announced that GigaOm has named the company a "Leader" and an "Outperformer" in its most recent report, the GigaOm Radar for Hybrid Cloud Data Protection for Large Enterprises.

An assessment of competing solutions, the GigaOm Radar report places Commvault in the Leaders circle of the Innovation/ Platform Play quadrant, highlighting its platform-driven approach with strong integration across the portfolio, a bestin-class BaaS (Backup-as-a-Service) experience, exceptional data management capabilities, and cyber resiliency features.

"Commvault's strong position in GigaOm's latest Radar report reaffirms our commitment to delivering secure, efficient,



and scalable data protection," said Param Kumarasamy, Vice President of Product Management, Commvault. "With Al-driven anomaly detection, threat mitigation, and risk analysis capabilities, we help customers improve their security posture across any hybrid cloud environment."

BEYONDTRUST ACHIEVES ISO 27001:2022 CERTIFICATION DEMONSTRATING COMMITMENT TO ROBUST CUSTOMER SECURITY

BeyondTrust, the worldwide leader in

intelligent identity and access security. has announced the company has achieved ISO 27001:2022 certification. The ISO 27001 standard applies a holistic management system approach to information security to address governance, organisation roles and responsibilities, processes, and technology to meet the business's information security risk management objectives. ISO 27001:2022 is the latest version of the international standard for Information Security Management Systems (ISMS), published by the International Organization for Standardization (ISO).

Aprio LLP, a nationally recognized business advisory and CPA firm, conducted the meticulous certification process.

As one of the first in its industry to obtain ISO 27001:2022 certification,

BeyondTrust demonstrates its commitment to preserving the security and confidentiality of sensitive information and customer data. Certification underscores BeyondTrust's comprehensive Information Security Management System (ISMS) of developing, operating, and administrating Privileged Password Management, Endpoint Privileged Management, and Secure Remote Access. BeyondTrust's deployment of cutting-edge technical controls, advanced encryption protocols, continuous monitoring, threat detection. robust incident response mechanisms, and routine security assessments work harmoniously to mitigate risk, while assuring customers that their entrusted data is shielded against cyber threats and unauthorised access.

"ISO 27001:2022 reflects enhancements and modernisation to the internationally



recognized ISO 27001:2013 information security standard," said Dan Schroeder, Leader of Information Assurance Services at Aprio. "We are excited and proud to serve as the ISO 27001 Certification Body for BeyondTrust as they leverage this important new standard to drive continuous improvement for security of their customer and other sensitive data amidst an everincreasing threat landscape."

SOLARWINDS CONTINUES ONGOING BUSINESS EVOLUTION WITH NEW AND UPGRADED SERVICE MANAGEMENT AND DATABASE OBSERVABILITY SOLUTIONS

SolarWinds, a leading provider of

simple, powerful, secure observability and IT management software, has announced the launch of new service management and database observability solutions designed to help companies achieve operational excellence, better business outcomes and accelerated innovation across the enterprise.

The new Enterprise Service Management (ESM) and upgraded SQL Sentry solutions are part of the company's ongoing transformative strategy to uniquely unify observability and service management. As a leader in enterprise software for nearly 25 years, SolarWinds provides customers with the tools they need to get maximum value from their digital innovation



efforts and increase productivity within complex IT environments. With a broad customer base across IT ops, DevOps, SecOps, AlOps, and CloudOps teams, SolarWinds has built on this success with transformative efforts to evolve its business, expand its product portfolio of industry-leading, AI-enabled solutions, and enhance its go-to-market strategy.

"As the challenges our customers face evolve, we are committed to evolving our solutions and business alongside them to ensure we consistently meet their needs," said Sudhakar Ramakrishna, SolarWinds President and CEO. "At SolarWinds, we have a simple but basic strategy for success: listening to, and learning from, our customers. Our foremost priority is helping our customers stay innovative, competitive, and productive. By giving them precisely the tools they need for today's most pressing challenges and keeping pace as they—and the industry transform, we've been able to grow, mature, and advance our own business."

VECTRA AI PLATFORM NOW AVAILABLE FOR PURCHASE ON THE CROWDSTRIKE MARKETPLACE

Vectra AI, the leader in AI-driven cyber

threat detection and response, has announced that the Vectra AI Platform with patented Attack Signal Intelligence is available in CrowdStrike's Marketplace, a one-stop destination and worldclass ecosystem of third-party security products. CrowdStrike Falcon customers can discover, try, buy and integrate the industry's first AI-driven, fully integrated hybrid attack detection, investigation and response platform.

The Vectra AI Platform works with the CrowdStrike Falcon® platform to provide customers integrated attack signal across public cloud, identity, SaaS, networks and endpoints arming SOC teams to keep pace with modern hybrid attacks. The newly released CrowdStrike Marketplace connects CrowdStrike to Vectra AI, a trusted integration to the Falcon platform, simplifying customers' security stacks, reducing their operational costs and helping to manage complexities seamlessly.

"As organisations shift to hybrid environments, they require solutions that enable them to keep pace with the evergrowing sophistication, speed and scale of hybrid attacks," said Kevin Kennedy, senior vice president of products at Vectra AI. "Now available for direct purchase in The CrowdStrike Marketplace, it's easier than ever for CrowdStrike customers to



procure the integrated attack signal our platform delivers and realise the promise of their extended detection and response (XDR) strategy."

CLOUDERA SIGNS STRATEGIC COLLABORATION AGREEMENT WITH AWS

Cloudera, the data company for trusted

enterprise Artificial Intelligence (AI), announced that it has signed a Strategic Collaboration Agreement (SCA) with Amazon Web Services, Inc. (AWS). This agreement strengthens Cloudera's relationship with AWS and demonstrates their commitment to accelerating and scaling cloud-native data management and data analytics on AWS. Through this agreement, Cloudera will leverage AWS services to deliver continuous innovation and lower customer costs with Cloudera's open data lakehouse on AWS for trusted enterprise generative AI.

As an AWS Independent Software Vendor (ISV) Workload Migration Program (WMP) Partner who also has a Cloudera Data Platform (CDP) Public Cloud listing available in AWS Marketplace, Cloudera makes it easy for customers to utilise credits to accelerate migrating workloads to the cloud and purchasing CDP on AWS.

Cloudera, with its focus on delivering



an enhanced open data lakehouse, has chosen AWS to run the most critical components of the CDP, including data in motion, data lakehouse, data warehouse, operational database, Al/machine learning, master data management and end-to-end security. This can help customers quickly migrate to CDP on the cloud without refactoring their applications while supporting hybrid deployments. Additionally, Cloudera has engineered CDP to integrate directly with AWS services, including Amazon Simple Storage Service (Amazon S3), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Relational Database Service (Amazon RDS) and Amazon Elastic Compute Cloud (Amazon EC2), providing customers with a tightly integrated platform that reduces cost and takes advantage of the latest innovations from AWS. Cloudera customers benefit from AWS native services without needing to manage the integrations themselves.



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+	20+	4000+	20+
Customers	Countries	Associates	Partnerships
USA Singapore A	Nalaysia Brunei Taiwc	an India Oman UAE	Qatar Saudi Arabia

www.bahwancybertek.com

UNLOCKING CYBERSECURITY EXCELLENCE

NED BALTAGI, MANAGING DIRECTOR – MIDDLE EAST, TURKEY AND AFRICA AT SANS INSTITUTE TELLS ANITA JOSEPH ALL ABOUT SANS GULF REGION 2023, THE LARGEST CYBERSECURITY TRAINING EVENT IN THE GCC.



ell us about SANS Gulf Region 2023. What can the security industry look forward to? Gulf Region 2023 is the

SANS Institute's largest cybersecurity training event in the GCC. We have a diverse range of courses scheduled for this event ensuring a holistic approach to cybersecurity education aimed towards helping narrow the skills gap in the Middle East. Professionals can look forward to hands-on training from global experts, as well as an opportunity to network with the cybersecurity community attending from across the globe.

What are some of the courses being taught at the event, and how is it expected to bridge the cybersecurity skills gap in the region?

It is vital that businesses, whether they are governmental entities or enterprises, take steps to protect their staff, data, and infrastructure by continually training their cybersecurity professionals across various cyber disciplines and the latest cybersecurity developments. There are 13 courses offered at SANS Gulf Region 2023, all meticulously designed with regional cyber requirements and best practices in mind, aimed to address the existing cybersecurity skills gap and build a bigger talent pool within the GCC – as well as educate and expand the proficiencies of visiting professionals from around the world.

The biggest threats that SANS Institute is helping organisations and professionals overcome are data breaches, malicious actors, and insider threats. Courses like FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics delve into investigative techniques and tools that equip defense professionals to detect, respond to, and mitigate cyber incidents effectively.

Attackers are expected to increase their focus on exploiting vulnerabilities in cloud-based infrastructures and applications, and SEC401: Security Essentials: Network, Endpoint, and

THE BIGGEST THREATS THAT SANS INSTITUTE IS HELPING ORGANISATIONS AND PROFESSIONALS OVERCOME ARE DATA BREACHES, MALICIOUS ACTORS AND INSIDER THREATS.

Cloud is an essential course for all cybersecurity practitioners. Offering foundational knowledge on network security, cloud defenses, and endpoint security, SEC401 ensures the very basics are covered. Enhancing awareness around cloud security in the Middle East is of the utmost importance in the current digital environment, as cloud security is constantly evolving, and organizations must stay ahead of the curve in order to protect their data and systems.

Moreover, to effectively deter threats and prevent hackers from infiltrating systems, a cybersecurity practitioner or team must first know and understand what it is they are preventing. SEC504: Hacker Tools, Techniques, and Incident Handling is a hands-on course diving deep into the world of hackers and the techniques they employ, coupled with incident handling procedures to detect, manage and mitigate threats.

Addressing the leadership and governance aspects of cybersecurity must also be a top priority for government leaders and cyber professionals. Courses such as MGT514: Security Strategic Planning, Policy, and Leadership provide insights on strategic planning, policy formation, and the legal facets of cybersecurity. Additionally, recognising the critical nature of industrial systems, courses such as ICS410: ICS/SCADA Security Essentials are designed to impart skills on securing critical infrastructure that powers the GCC region.

The breadth of courses ensures that professionals in the Middle East can fill in their knowledge gaps extensively. By equipping people across these various domains, we hope to overcome the talent shortage and create a robust and resilient cybersecurity ecosystem in the Gulf region.

Give us a background about the instructors teaching this course.

SANS prides itself on having a rigorous instructor selection process. All our instructors are seasoned professionals and globally recognised experts in their respective fields. Our instructors have often faced and overcome the very challenges they teach about, giving them a unique vantage point. With a blend of academic prowess and real-world experience, they bring to the table a wealth of knowledge, ensuring that attendees receive not just theoretical instruction but also practical insights that can be immediately applied in their professional settings.

What SANS courses are the most popular and why?

Effective security requires a balance between detection, prevention, and response capabilities and courses that encapsulate all three of these principles have seen the most traction. Over the years, network security courses such as SEC501 (Advanced Security Essentials) have seen high demand as security teams of all sizes want to enhance their understanding and skills in the specific areas of network architecture defense, penetration testing, security operations, DFIR, and malware analysis. SEC530 (Defensible Security Architecture and Engineering) is also popular as it helps professionals build and maintain a layered security infrastructure across hybrid environments while implementing Zero Trust pillars. Meanwhile, SEC497 (Practical Open-Source Intelligence) remains a top choice for students, providing actionable information and techniques to help individuals perform open-source intelligence (OSINT) research safely and effectively. 1

UNIFIED MANAGEMENT IS KEY TO SINGLE VENDOR SASE

SATISH MADIRAJU, FORTINET



t's no secret that SASE has skyrocketed in popularity in recent years due in large part to how the solution provides strong threat protection and secure access no matter where a user, device, or application is located. This is no small feat, especially in the work-fromanywhere (WFA) era, where employees are logging in from a coffee shop one day and the office the next.

Because of the popularity of SASE, many vendors are trying to get a piece of the pie and are making strong claims about their offerings that may fall short in practice. One of the most misunderstood SASE features is unified management, which empowers organisations with a simple management console for their entire solution—both the networking and security components. Because this is such an important element of any SASE deployment, customers need to understand how to cut through the marketing chatter and procure the best solution for their needs.

Single-Vendor SASE, Please

SASE is one of the first truly converged networking and security solutions that has gained mainstream popularity. But, one of the biggest challenges facing customers is understanding all of the networking elements and clouddelivered security services that work together to provide all SASE features across the entire hybrid network. At first, many organisations used point products from multiple vendors for SASE functionalities. This presented significant policy enforcement and management challenges because these products all used different management dashboards and didn't share information. IT teams were bogged down trying to manage the complexity and costs of working with multiple vendors.

Because of these issues, industry leaders began promoting single-vendor SASE, which is when a single company supplies both the networking and cloud-



delivered security components. One of the major selling points for single-vendor SASE is unified management, which describes a simple-to-use management tool for all security and networking features.

Before single-vendor SASE, IT professionals had to update security policies on many point products. Now they can upload the new policy to a management console and deploy it across all relevant areas with a few clicks.

Understanding Unified Management

Now, when someone says "unified management," I'm sure you have a cursory idea of what it means. But what does it entail when it comes down to brass tacks? Unified management should mean a single management console for the entire SASE solution. This single console provides end-to-end visibility and the ability to streamline policies.

However, some vendors claim to offer a single-vendor solution with unified management when they really require customers to work with separate management tools. This often happens if a vendor acquires a company or companies to combine with their current offerings to provide SASE. Essentially, this is a single company selling two solutions under a single name when the elements work in silos and have to be managed as such. Of course, streamlining management down to two consoles when some vendors were using five or more is an improvement, but it undermines the true value of unified management.

And this is not a minor point. Having a single console to deploy policies, manage

SASE IS ONE OF THE FIRST TRULY CONVERGED NETWORKING AND SECURITY SOLUTIONS THAT HAS GAINED MAINSTREAM POPULARITY. network traffic, and ensure a positive user experience is crucial. A customer told me, "Being able to manage and address everything from a single location increases our efficiency and our ability to deploy and manage and address issues with limited staff."

Going Beyond SASE

A SASE offers a more streamlined and efficient way to manage and secure network traffic and is well-designed to handle and protect the hybrid workforce. However, remember that not all SASE solutions are built the same. I recommend you partner with a provider with deep SASE experience and a truly unified offering.

And remember that while unified management is key for SASE, it's also critical for other components of your security architecture as well. Having a single console that provides visibility and control for the entire hybrid network, including LAN/WLAN, IoT, OT, data centers, and more, empowers organisations with the information they need to protect their business and roll out updates efficiently.

UNIFIED EXCELLENCE: ACHIEVING SEAMLESSNESS IN APPLICATION QUALITY & SECURITY

RAISA MAHOMED, ASSOCIATE VICE PRESIDENT, BAHWAN CYBERTEK

n the fast-paced world of digital business, software development is the bedrock of innovation and growth. Historically, the need for rapid software delivery would overshadow essential aspects like software quality and security. Today, with enterprises embracing digital transformation at a pace like never before, security is no longer an afterthought. It is a boardroom priority.

Future Fit. customer-centric enterprises must deploy an approach that seamlessly integrates application security and software testing. Comprehensive testing to detect bugs and vulnerabilities should complement rapid software delivery. Security should become a top priority if businesses want to protect themselves from cyber threats, stay compliant with industry regulations, and ultimately enhance experience for end users. Software security in the digital era, however, can be complicated. Coordinating multiple tools for testing and security can be a logistical nightmare, leading to inefficiencies and delays. Staying compliant with industry regulations poses yet another challenge as requirements continually evolve. So, how can enterprises build a resilient Software Development Life Cycle (SDLC)?

Enter Bahwan CyberTek's revolutionary approach, designed not only to streamline the SDLC but also to enhance software quality and reinforce security. Investing in our solution offers an array of benefits. First, our unified solution simplifies development by bringing software testing and application security together under one roof, eliminating the need to juggle multiple tools. This consolidation facilitates a smoother transition in the software development journey.

Second, our advanced tooling covers all aspects, from functional to performance



testing, ensuring that the software meets the highest quality standards. With continuous monitoring and threat detection, security is maintained around the clock. Furthermore, our solution is tailored to help enterprises effortlessly meet industry regulations and standards, ensuring the organization remains compliant.

Lastly, by merging software testing and application security, we significantly reduce vulnerability and security breach risks, safeguarding the enterprise and its reputation. This streamlined approach accelerates software delivery, giving a competitive edge. Moreover, it eliminates the need to manage numerous tools, resulting in substantial cost savings. Delivering secure, high-quality software fosters trust with customers, leading to increased loyalty and a positive brand image.

In today's digital landscape, compromising on software quality or security is no longer an option. At Bahwan CyberTek, we are committed to helping organizations achieve unparalleled benefits across the software development journey, ensuring a seamless transition from development to deployment. IN PARTNERSHIP WITH



🛞 tahawultech.com

PRESENTS



18TH OCTOBER 2023

HABTOOR PALACE DUBAI, LXR HOTELS & RESORT

#tahawultech #CXOSummit2023 #CirrusLabs



REGISTER NOW

The **CXO Summit** is a forum during the week of **GITEX GLOBAL** '23 that has been designed to network, share, learn, and build the future that will help organizations navigate and overcome the complexities that exist in our ever-evolving digital economy.

Together, we can simplify the path to digital success.

Your journey is our journey.



OFFICIAL PUBLICATIONS

Reseller



HOSTED BY

🚸 tahawultech.com

ORGANISED BY

For more information about the event, please visit https://www.tahawultech.com/cxo-summit/2023/



THE GAME CHARGER BERNARD MONTEL, EMEA TECHNICAL DIRECTOR AND SECURITY

BERNARD MONTEL, EMEA TECHNICAL DIRECTOR AND SECURITY STRATEGIST AT TENABLE TELLS ANITA JOSEPH HOW AI IS RESHAPING THE THREAT-SECURITY LANDSCAPE AND HOW TENABLE IS DRIVING THIS CHANGE.

an you explain the new generative AI capabilities and services introduced by Tenable with the launch of ExposureAI?

Tenable has, for years, harnessed artificial intelligence (AI) and machine learning (ML) in multiple ways across its solutions. This includes enhancing models around asset criticality assessment, in prioritisation techniques, and other methods we use to differentiate our offerings and add valuable insight for customers.

With the launch of Exposure AI we take this even further. ExposureAI is how Tenable uses AI (generative artificial intelligence, deep learning, AI and machine learning) to fuel our exposure management capabilities with the following use cases:

- Explain: Derive succinct guidance to better understand product findings.
- Search: Simplify search across your asset inventory for complete visibility.
- Action: Proactively deliver insights for actions with the most impact.

How does the Tenable Exposure Graph, powered by Snowflake, contribute to the functioning of the ExposureAI engine?

If you have unique data then you're

going to have unique intelligence guiding decisions. It's truly "garbage in, garbage out" - or "gold in, gold out" - depending on the source. Tenable's exposure data stands as the world's largest repository of contextual exposure data, fueling the capabilities of Tenable ExposureAI. This unified data platform - representing more than 1 trillion unique exposures, IT assets and security findings (vulnerabilities, misconfigurations and identities) across IT, public cloud and OT environments is the largest repository of contextual exposure data in the world and feeds all of Tenable's Exposure Management products.

With leading breadth and depth of data and context, Tenable empowers

INSTEAD OF WAITING TO BE ATTACKED AND THEN RESPONDING, IT'S VITAL THAT SECURITY TEAMS TAKE A PREVENTIVE APPROACH TO CYBER DEFENCE. organisations with comprehensive exposure management across the everexpanding attack surface. It provides a wealth of information, enabling organisations to gain valuable insights into potential vulnerabilities, threats and misconfigurations.

How does Tenable ensure the accuracy and reliability of the insights generated by ExposureAI, considering the constantly evolving threat landscape?

Harnessing AI efficiently requires data and expertise to generate meaningful insights and Tenable leads the charge in exposure management with AI as a part of our DNA. While AI is capable of quickly identifying and automating some actions that need to be taken, it's imperative that humans are the ones making critical decisions on where and when to act. Our expert team of data scientists boasts 40+ patents, 40+ high-profile journal publications, five have been awarded PhDs and the team has unparalleled experience in machine learning across diverse industries. Couple this with the dynamic data they have at their fingertips 1 trillion counts of threat, exposure and asset data, 1 billion assets, 60 billion exposure events and 800 million security configurations for comprehensive data-



driven insights that are constantly being enhanced with additional intelligence.

ExposureAl transforms how security teams prevent successful attacks, empowering lightning-fast analysis, decision-making and guidance with the power of generative Al. It searches for patterns, explains what's found in the simplest language possible, that helps security teams decide what actions to take to reduce cyber risk. When harnessed by defenders it will cut through complexity to provide the concise guidance defenders need to stay ahead of attackers and prevent successful attacks.

Can you explain how Tenable's generative AI capabilities can help security teams be more efficient and focus more resources on preventing successful attacks?

For far too long security teams have been treating the symptoms of cybercrime rather than curing the disease. The current approach is reactive and relies heavily on post-event data to find the origin of an attack and clean up the mess. This modus operandi is a losing battle against asymmetric cybercriminal activity where defenders need to be right 100% of the time and threat actors only once.

Instead of waiting to be attacked and then responding, it's vital that security teams take a preventive approach to cyber defence. The need to understand your attack surface and proactively manage risk to the business has never been more urgent. The only way to stay ahead of the curve is to find the weak spots in defences proactively, before attackers can, and prioritise remediations based on organisational risk.

Leveraging comprehensive data and expertise, powered by Exposure AI, Tenable helps teams shift from reactive to proactive, turning all analysts into expert defenders to reduce risk across their evolving attack surfaces — no matter where threats may come from.

How does Tenable's generative Al differentiate itself from other Al-driven solutions in the cybersecurity market?

If you have unique data then you're going to have unique intelligence guiding decisions. It's truly "garbage in, garbage out" — or "gold in, gold out" — depending on the source. Equally important is training the algorithm to remove false positives, and the larger the dataset the more intelligence there is to work with. Tenable's exposure data stands as the world's largest repository of contextual exposure data, fueling the capabilities of Tenable ExposureAI.

Can you share any insights on the future of generative AI in cybersecurity and how it may continue to evolve in the coming years?

For security teams and organisations, generative AI is the same as any other new technology that enters the arena. While created as a tool for good, AI can just as easily be weaponized by malicious cyber attackers to accelerate their money making schemes or even create misinformation and we need to keep one step ahead.

There is a learning curve and we're on the cusp of understanding what AI is capable of. With generative AI — such as Google Virtex AI, OpenAI GPT-4, LangChain and many others — it is possible to return new intelligent information in minutes in simple language even non-technical people can understand. For security, these insights will continue to become more accessible and capable of turning anyone into expert defenders.



CYBERSECURITY FOR ALL.

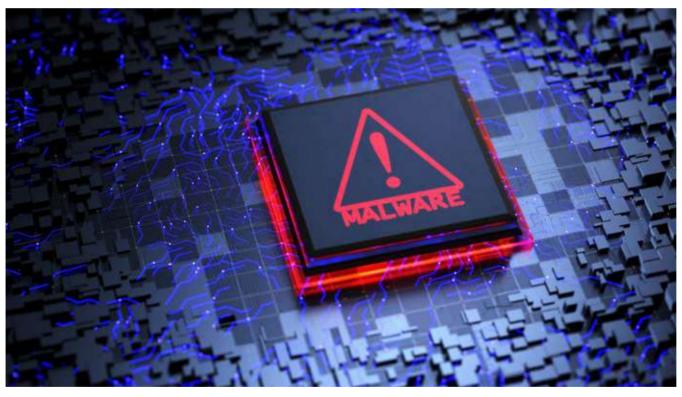
All threats, all businesses, all people.

Get fierce defenses for a world of complex threats.

Barracuda.com

Barracuda will be at GITEX Global 2023 Booth: H24 - C50

CHINESE MALWARE APPEARS IN EARNEST ACROSS CYBERCRIME THREAT LANDSCAPE: PROOFPOINT



ince early 2023, Proofpoint has observed an increase in the email distribution of malware associated with suspected Chinese cybercrime activity. This includes the attempted delivery of the Sainbox Remote Access Trojan (RAT) – a variant of the commodity trojan Gh0stRAT – and the newly identified ValleyRAT malware. After years of this malware not appearing in Proofpoint threat data, its appearance in multiple campaigns over the last six months is notable.

The phrase "Chinese-themed" is used to describe content related to this malicious activity, including lures, malware, targeting, and metadata that contains Chinese language usage.

Campaigns are generally lowvolume and are typically sent to global organizations with operations in China. The email subjects and content are usually written in Chinese, and are typically related to business themes like invoices, payments, and new products. The targeted users have Chinese-

《发票信息》

○ 用友发票 <lwplbh@cluedk.com>

尊敬的客户: 您好! 您的增值税电子发票已成功开具,发票详情如下: 发票代码: 052002100211 发票号码: 26866498 发票详情信息 26866498.zip (469.95KB) 电子发票版式文件下载地址: http://rus3rcqtp.hn-bkt.clouddn.com/26866498.zip

(温馨提示:此文件保存期为15天,请您尽快下载。) Suggestion: The storage period of this attachment is 15days. Please download it as soon as possible.

language names spelled with Chineselanguage characters, or specific company email addresses that appear to align with businesses' operations in China. Although most campaigns have targeted Chinese speaking users, Proofpoint observed one campaign targeting Japanese organisations, suggesting a potential expansion of activity.

These recently identified activity clusters have demonstrated flexible delivery methods, leveraging both simple and moderately complex techniques. Commonly, the emails contain URLs linking to compressed executables that are responsible for installing the malware. Proofpoint has also observed Sainbox RAT and ValleyRAT delivered via Excel and PDF attachments containing URLs linking to compressed executables.

Research into additional activity clusters utilising these malwares demonstrate enough variety in infrastructure, sender domains, email content, targeting, and payloads that researchers currently conclude that all use of these malwares and associated campaigns are not attributable to the same cluster, but likely multiple distinct activity sets.

The emergence and uptick of both novel and older Chinese-themed malware demonstrates a new trend in the

overall 2023 threat landscape. A blend of historic malware such as Sainbox – a variant of the older Gh0stRAT malware – and the newly uncovered ValleyRAT may challenge the dominance that the Russian-speaking cybercrime market has on the threat landscape. However, the Chinese-themed malware is currently mostly targeted toward users that likely speak Chinese. Proofpoint continues to monitor for evidence of increasing adoption across other languages.

With this resurgence of Chinese themed malware, the questions arise: is the impact of older malware easier to detect due to its age? Does mature detection always mean mature security? Based on Proofpoint's analysis, the answer is not necessarily, as older malware can still be effective, especially when threat actors constantly change tactics by rotating IPs, domains, encoding, and obfuscation. Consequently, even though these malware families are not new, organizations cannot afford to underestimate the risk they pose.

Today at 5:39 am

Proofpoint research suggests that this activity does not seem to be related to a single entity but rather appears to be a cluster of activities based on temporal patterns. The appearance of ValleyRAT alongside the older families hints at the possibility of their relation in terms of timing. Proofpoint anticipates ValleyRAT will be used more frequently in the future.

Raising awareness in 2023 about the reappearance of these threats serves as an informational bulletin for the community. While new and sophisticated threats seemingly dominate the daily threat landscape, it is essential to maintain a balanced perspective by acknowledging seemingly less significant risks that persist. Despite being neither new nor advanced, Sainbox RAT still poses a threat in 2023, and ValleyRAT is an emerging threat in this space.



aspers THE FUTURE OF CYBERSECURITY

RASHED AL MOMANI, GENERAL MANAGER OF MIDDLE EAST AT KASPERSKY, TELLS ANITA JOSEPH HOW THE COMPANY IS LEADING INNOVATION IN CYBER IMMUNITY AND HELPING GOVERNMENTS TO STAY ONE STEP AHEAD OF THREAT ACTORS WITH THREAT INTELLIGENCE.

hy is the government sector in the Middle East a prime target for Advanced Persistent Threats (APTs)? How can government entities turn their security shortcomings into opportunities?

The government sector stores a high volume of sensitive data which is lucrative for cybercriminals. Over the past two years, Kaspersky experts have been monitoring 17 APT groups actively targeting the UAE. Their top targets continue to be the governmental and diplomatic institutions, military and defence, and finance. APT groups are known for their capability to develop sophisticated tactics that allow them to remain stealthy and unnoticed for long periods of time. This has made them notorious for launching ransomware attacks, committing cyber espionage and financially-motivated cybercrime.

Although governments have set protocols and policies in place to defend themselves against such cyberattacks, visibility across all functions is extremely important. Lack of visibility can be a shortcoming.

Turning this shortcoming into an opportunity is possible if governments have the power of knowledge. This is

AT GITEX WE ARE ANNOUNCING THE LAUNCH OF KASPERSKY CONTAINER SECURITY → (KCS), A FULL-FEATURED SOLUTION FOR CONTAINER DEVELOPMENT ENVIRONMENTS. where Kaspersky's Threat Intelligence comes into play. With this service, governments can access expertise and insights on cybercriminal tactics, history and motives to better understand their mindset and stay one step ahead. For example, a telecommunications organisation in the UAE using our Threat Intelligence platform can have access to insights on APTs targeting other telecommunications companies in the region. This information can be analysed and used to strengthen the foundation of their cybersecurity infrastructure to protect their people, data, and assets better.

What is Kaspersky doing different this year at GITEX Global 2023?

At the beginning of October, we launched Kaspersky SD-WAN in some countries in META thus making one important step towards building the SASE model that stands for network and security services synergy and aims to provide agile and reliable networks, while shifting from different security solutions to unified security available from private or public cloud. This new solution helps geodistributed companies build reliable networks, managing them from a single console, and connect new branches with a zero-touch experience.



We are also announcing the new release of Kaspersky Industrial CyberSecurity (KICS), an Extended Detection and Response (XDR) platform for industrial enterprises. With significant advancement in XDR capabilities we help to achieve complete Industrial Automation and Control Systems (IACS) visibility. And with new security audit feature it's now easy to implement automated controls to ensure compliance with best industry standards and practices.

At GITEX we are also announcing the launch of Kaspersky Container Security (KCS), a full-featured solution for container development environments. The solution helps to detect vulnerabilities, malware, sensitive data and misconfigurations in images, while providing security for all the stages of containerised application development. It can strengthen DevOps protection both for companies with developed DevSecOps processes and for companies that only begin to implement them.

Kaspersky is the first private company in the world that has its own ICS CERT team. What prompted Kaspersky to establish an ICS CERT team?

Kaspersky's ICS CERT keeps a close eye on the critical infrastructure sector. Our recent ICS CERT report findings reveal that in the first half of 2023, 36.8% of attacks were detected on ICS computers in the Middle East, which is higher than the global average of 34%. The most attacked industries were energy, oil & gas, and manufacturing.

Organisations in the critical infrastructure sector can consider these numbers as a cautionary tale to increase their level of cyber readiness. This is



true for our region, especially because the energy, oil & gas, and manufacturing industries form the backbone of the economy and are often the prime targets. A cyberattack on these sectors can have irrecoverable consequences, and there are many examples worldwide that have served as valuable lessons. Today, the risk has further increased, considering these industries are rapidly digitising by embracing automation and IoT technologies into their operations. Another point of discussion is the failure on the part of organisations to understand that Information Technology (IT) is different from Operational Technology (OT). So, OT managers cannot be considered as IT managers. This gap between existing skills and expertise is bridged by Kaspersky's ICS CERT.

Kaspersky's ICS CERT monitors, and analyses an organisation's current level of cyber readiness. The team carries out assessment of security products, identifies vulnerabilities and provides organisations with recommendations to eliminate risks. Kaspersky's ICS CERT also creates methodologies, standards, and frameworks for secure-by-design technologies to safeguard industrial organisations.

WE ARE ALSO ANNOUNCING THE NEW RELEASE OF KASPERSKY INDUSTRIAL CYBERSECURITY (KICS), AN XDR PLATFORM FOR INDUSTRIAL ENTERPRISES.

Kaspersky has created and is pioneering the Cyber Immunity approach. Do you have cyber immune products available in the region?

We believe that Cyber Immunity is the future of cybersecurity. The exponential growth of IoT in the critical infrastructure sector, also dialled up the level of cyber vulnerabilities. We saw this as an opportunity to launch Kaspersky IoT Secure Gateway 100 and Kaspersky IoT Secure Gateway 1000, the first of our cyber immune products.

Both products are based on KasperskyOS, and are designed to serve as a secure gateway for the Internet of Things in an industrial network. The gateway connects IoT devices and controllers with business applications and cloud platforms. It then ensures that interactions between devices and platforms, and data transfers are secure with its network attack protection capabilities.

Recently we have entered into a partnership with Centerm, and will

ONE WAY FOR ORGANISATIONS TO COMBAT LACK OF SECURITY SKILLS IS TO LEVERAGE EXPERT SOLUTIONS LIKE THE KASPERSKY MANAGED DETECTION AND RESPONSE (MDR).

provide cyber Immune thin clients worldwide. This is the world's first thin client that does not requires additional antivirus protection tools, and will be available in the Middle East next year. The Kaspersky Thin Client is designed to provide users with access to a remote desktop and serves as a substitute for a local workstation. It can be efficiently used in organisations with a large branch network and geographically distributed structure. Government, commercial structures, transport and industrial enterprises, financial institutions and retail, smart city infrastructure, as well as in the industrial automation industry can

implement this thin client with ease. Good to mention that this partnership started last year with a MOU signed at GITEX and grew into a big OEM-contract with the world's leading thin client manufacturer.

Talent too plays an important role in ensuring cybersecurity strategies are successful. How should organisations bridge the evident skills gap in the cybersecurity industry?

Like other economies worldwide, the Middle East is facing a shortage of cybersecurity talent, more so in the critical infrastructure sector. According to Kaspersky telemetry, 66%

THE GATEWAY ENSURES THAT INTERACTIONS BETWEEN DEVICES AND PLATFORMS AND DATA TRANSFERS ARE SECURE WITH ITS NETWORK ATTACK PROTECTION CAPABILITIES. KISG 100 is a software/hardware system based on KasperskyOS, and is designed to work as a secure gateway for the Industrial Internet of Things in an enterprise network.



of industrial organisations have faced significant security staffing challenges. We continue to work closely with organisations, government entities and universities to train, teach and hone new and existing talent, and raising the bar of cyber readiness.

One way for organisations to combat lack of security skills is to leverage expert solutions like the Kaspersky

$\begin{array}{l} \textbf{CYBER IMMUNITY}\\ \rightarrow \textbf{ IS THE FUTURE OF}\\ \textbf{CYBERSECURITY.} \end{array}$



KISG 1000 is powered by the KasperskyOS operating system. It both collects data from IoT devices and helps provide reliable cybersecurity based on the Kaspersky Cyber Immunity approach.

Managed Detection and Response (MDR). With MDR, organisations get access to our experts round the clock, and are provided with tailored ongoing detection, prioritisation, investigation and swift response to incidents. This service is already present in our region, and will soon be available in Saudi Arabia through a local partnership. The launch of MDR will also strengthen our data sovereignty efforts in the region.

Having said that, the Kaspersky Threat Intelligence platform is also a rich knowledge platform that can immensely contribute to training workshops. The platform provides IT teams with easy access to Kaspersky's expertise and deep intelligence on every aspect of cybersecurity. IT teams can understand and learn from the latest cyber developments and advancements, and in parallel support the organisation to develop their cybersecurity measures on technical, tactical, operational and strategic fronts. **1**

CISO 50 & FSA AWARDS 2023



Celebrating THE STARS

he security industry has always been in a never-ending race against its adversaries, but in the last three years in particular, the rate of change has accelerated. While companies continue to invest in new and emerging technologies and layer more

systems into their IT networks, this has resulted in potential new vulnerabilities, and adversaries have been leveraging powerful, integrated tools and capabilities with artificial intelligence and machine learning to cause irrevocable loss of critical data and information. The scope of the threat is growing, and no organisation is immune. In fact, the unfortunate reality is that even today's most sophisticated cyber controls, no matter how effective, will soon be obsolete.

The CISO 50 & Future Security Awards were introduced keeping in mind this dynamic threat-security scenario. These awards recognise decision makers, businesses and vendors that have risen above challenges and delivered groundbreaking business value through innovative application of security technologies. It seeks to honour industry visionaries who have shown dedication and prowess in creating a cyber secure world. It acclaims the best security minds and projects in the region whose technologies, products or solutions are deemed to have significant potential in meeting the needs of the rapidly transforming digital era.

The evening of September 12th saw a glittering array of cybersecurity visionaries, experts and decision makers come together at the Taj Exotica Resort & Spa, the Palm, to celebrate excellence and innovation. Sponsored by Cloud Partner – SolarWinds, Gold Sponsors – Barracuda Networks, LinkShadow, MMA Infosec, Resecurity, StarLink and Silver Sponsor – CyberHub 24/7 CSOC Powered by Finesse, this prestigious event celebrated excellence and innovation in the field of cybersecurity and provided a unique platform for networking, knowledge sharing and recognising outstanding contributions to the industry.

The highlight of the evening was an insightful panel discussion titled "The Shifting Security Horizon: Challenges and Opportunities." Experts from various sectors of the cybersecurity industry engaged in a dynamic conversation, sharing their experiences and insights on the evolving landscape of cybersecurity, particularly in the area of security investments. The panel delved into the latest threats and trends, the role of artificial intelligence and machine learning in cybersecurity, and strategies for staying ahead of cyber adversaries.

The panelists included:

- Amit Mehta, Cybersecurity Consulting Practice Lead

 EEMEA, Mastercard
- 2. Anoop Kumar Paudval, Information Security Manager, Al Nisr Publishing
- **3. Ashish Khanna,** Global Head of Information Security, Sharaf Group
- 4. Mhd Wail Khachfa, Chief Information Security Officer and Business Continuity Manager, Digital Ajman
- Rajesh Yadla, Director Head of Information Security, Al Hilal Bank
- 6. Waqas Haider, Chief Information Security Officer, HBL Microfinance Bank
- Moderated by Anita Joseph, Editor Tahawultech. com and Security Advisor, the engaging discussion shed light on the challenges and opportunities faced by organizations today in the realm of cybersecurity. Attendees left the session with a deeper understanding of the ever-evolving threat landscape and actionable insights to bolster their security strategies.

tahawultech.com CISO50 AWARDS 2023





CISO 50 & FSA AWARDS 2023



tahawultech.com CISO50 AWARDS 2023



Shijin Prasad Cure Medical Centers, Al Nokhba Medical Centers & Cure Pharmacies



Osama Abbas Emirates Transport



HBL Microfinance Bank Ltd





Ala Asali Arab National Bank



Mukesh Kumar Apparel UAE



Ahmed Nabil Mahmoud Abu Dhabi Islamic Bank



AD Ports



Munish Jain Dubai Health Authority (DHA)



Wajahat Hussain Etihad Airways



tahawultech.com CISO50 AWARDS 2023



Sunil Kumar Sharma Aldar Properties



Abhilash Radhadevi OQ Trading

FIMEDIAGROUP.COM



Gigi Mathew Thomas Ittihad International Investment LLC



Divij Verma Mashreq Bank



Umesh Moolchandani Bin Dasmal Group



Nishanth Menothparambil Enova Facilities Management Services

CISO 50 & FSA AWARDS 2023







Sunil Kumar Nair Al Ain University



Digital Ajman

tech UJF

Hamda AlMaazmi Ministry of Health and Prevention - MOHAP



Hamed Obaid Sebait Naseib Areidat Central Bank of the UAE

DIA GROUP



Prabhat Kumar Pathak Gulf Marketing Group





Jinson Pappachan Emirates Policy Center



Eng. Eissa Naser Al Hammadi Department of Health Abu Dhabi



Anoop Kumar Paudval Al Nisr Publishing LLC



Nesto Group



tahawultech.com CISO50 AWARDS 2023



Mohannad Hennawi NAFFCO







Padam Kafle Aster Hospitals Jeevan Badigari DAMAC Group Hasnain Juzer Ali Saudi German Health UAE Mohamed Riyasudeen Al Ain Ahlia Insurance Co (PSC) Zaheer Shaikh Al Maryah Community Bank LLC Velmurugan Segamani **Emaar Properties PJSC** Dubai Government - Legal Affairs Department Anas Eltahir Mohamed Gazzaz Tonomus Phil Westgarth Network International Adel Alhosani Dubai Customs Abbas Sabuwala DMCC Authority Sarith Bhavan Mubadala Investment Company

CISO 50 & FSA AWARDS 2023













tahawultech.com FUTURE SECURITS AWARDS 2023





Best Data Analytics Vendor of the Year SAS

Best Network Management Solutions for SMBs of the Year Nuclias by D-Link



Best Security Solutions Provider of the Year Cloud Box Technologies



Best Security VAD of the Year StarLink



Best Cybersecurity Solutions Partner of the Year CNS Middle East



OPSWAT

CISO 50 & FSA AWARDS 2023



tahawultech.com FUTURE SECURITY AWARDS 2023



Best Managed Security Services Provider of the Year Help AG





Best Cloud Application Security Vendor of the Year Barracuda Networks

Best Anti-DDoS Vendor of the Year A10 Networks



Best Cloud Security Vendor of the Year Cloudflare



Raqmiyat





Veeam Software

Best Network Security Vendor of the Year Juniper Networks

ahawult

Resecu

Ba

1

CISO 50 & FSA AWARDS 2023



tahawultech.com FUTURE SECURITY AWARDS 2023



Best Digitalisation & Cybersecurity Provider of the Year Bahwan CyberTek





Best Network for Digital Video Surveillance Systems of the Year Allied Telesis

Best Intelligent NDR Vendor of the Year LinkShadow



Best Privelege Access Management Vendor of the Year Delinea



Best Security Systems Integrator of the Year MMA Infosec





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

Thank You Sponsors

CLOUD PARTNER



GOLD SPONSORS

Barracuda







SILVER SPONSOR

YBERHUB 24x7 CSOC POWERED BY 🚸 FINE(SE

#CISO50FSA2023 #tahawultech



22 – 24 MAY 2024

"GITEX AFRICA reflects the importance of the continent's tech sector on the world stage".

His Highness Sheikh Hamdan Bin Mohammed Bin Rashid Al Maktoum

Crown Prince of Dubai and Chairman of The Executive Council of Dubai

"The Continent's Most **Important Tech Show**"



Get involved, visit us at CC2-11 at GITEX GLOBAL, Dubai World Trade Centre & H2-F60 at EXPAND NORTH STAR, Dubai Harbour

MAIN

FEATURING

GITEX AFRICA 2024 creating a bold future for Africa

- Smart Manufacturing Agritech Ai Everything Consumer Tech Cyber Security
 - Digital Finance Digital Cities Telecom/Infrastructure Startups

UNDER THE AUTHORITY OF

y Of Digital Tr

HOSTED BY

Digital Development Agency

ORGANISED BY



AFFILIATED WITH

GLOBAL

gitexafrica.com #gitexafrica

Smart security for every home.

Ring lets you monitor every corner of your property. With a Video Doorbell at your door, Security Cameras and Alarm system 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

To learn more, visit us at GITEX Global 2023 Stand H20-B05



SPECIAL REPORT:

LINKSHADOW PATRICK RAMSEYER, VP, EMEA

6

SPECIAL REPORT: LINKSHADOW



he Cyberthreat Landscape

The modern cybersecurity landscape is a battleground where cybercriminals continually innovate and adapt their tactics to exploit vulnerabilities. Traditional security measures, while effective to some extent, often fall short in the face of sophisticated threats. This dynamic environment demands a holistic, forward-looking approach that can identify and respond to threats before they cause significant damage. In fact, the current cyberthreat and security landscape presents a complex and ever-evolving challenge for organisations worldwide. As technology advances, so do the tactics and techniques employed by cybercriminals. In recent years, the cyberthreat-security landscape has become particularly challenging, with attacks becoming more rampant, diverse and highly organised. Some key trends and threats shaping this landscape include:

Ransomware: Ransomware attacks have surged, with cybercriminals targeting organisations of all sizes. Attackers

encrypt critical data and demand ransom payments in exchange for decryption keys, crippling businesses and causing substantial financial losses.

Supply Chain Attacks: Cybercriminals are increasingly targeting the supply chain to infiltrate organisations. Breaching a trusted supplier can provide access to multiple targets, making these attacks especially dangerous.

Nation-State Threats: Nation-states continue to engage in cyber espionage and cyber warfare. These attacks can have far-reaching consequences, disrupting critical infrastructure and posing national security threats. Insider Threats: Malicious or nealigent

insiders remain a significant concern. Employees with access to sensitive data can inadvertently or deliberately compromise security.

AI-Powered Attacks: The use of artificial intelligence in cyberattacks is growing, allowing attackers to automate tasks, evade detection, and target vulnerabilities more effectively.

Challenges in Securing Critical Assets Securing critical assets in this evolving landscape presents several formidable

LINKSHADOW'S COMMITMENT TO SECURITY IS UNWAVERING, AND IT PLACES PARAMOUNT EMPHASIS ON CUSTOMER INPUT.

challenges for businesses: **Resource Constraints:** Many organisations struggle to allocate sufficient resources to cybersecurity efforts. Smaller businesses may lack dedicated cybersecurity teams, while larger enterprises may face budget constraints despite recognising the importance of cybersecurity.

Rapidly Changing Threats: Cyber threats evolve at a breakneck pace. Keeping up with the latest attack techniques and vulnerabilities is a constant challenge for security professionals.

Complexity of IT Environments:

Modern organisations have complex IT infrastructures, including on-premises, cloud, and hybrid environments. Securing these diverse systems and ensuring they work together seamlessly is challenging.

Trust-security balance: Managing insider threats is tricky, as organisations must balance trust and security. Implementing effective controls without stifling productivity can be a delicate balancing act.

Vulnerability Management: Identifying and patching vulnerabilities promptly is crucial. However, businesses often struggle with vulnerability management due to the sheer number of systems and applications they must monitor.

Regulatory Compliance: Navigating the complex landscape of cybersecurity regulations and compliance requirements is a significant challenge. Failure to comply can result in severe penalties.

Skills Gap: There is a shortage of skilled cybersecurity professionals. Recruiting and retaining talent is difficult, leaving many organisations understaffed and vulnerable.

Third-Party Risks: Businesses often rely on third-party vendors and service providers. However, these relationships can introduce security risks if vendors do not prioritize cybersecurity.





Security Awareness: Human error remains a leading cause of security breaches. Educating employees about cybersecurity best practices is essential but can be challenging.

Zero-Day Vulnerabilities: Cybercriminals are continually searching for unknown vulnerabilities (zero-days) to exploit. Businesses must be prepared for attacks that target these vulnerabilities before patches are available.

The current cyberthreat and security landscape demand constant vigilance and adaptation from businesses. Cybersecurity is no longer an option; it is a necessity to protect critical assets and safeguard organisational reputation. Meeting these challenges requires a multifaceted approach, including investment in technology, personnel, and training, as well as collaboration with industry peers and regulatory bodies. Ultimately, securing critical assets in today's digital world is an ongoing battle that organisations must be prepared to fight.

Enter LinkShadow

LinkShadow, founded by a team of

Identity Intelligence

cybersecurity experts, recognised the pressing need for a comprehensive solution that could address the challenges of the contemporary threat landscape. Established at a time when businesses were grappling with escalating cyberattacks, LinkShadow aimed to empower organisations with the tools and insights necessary to stay ahead of cybercriminals.

What sets LinkShadow apart is its holistic approach to cybersecurity. Instead of relying on siloed security solutions, LinkShadow offers an integrated platform that provides end-to-end visibility into an organisation's digital ecosystem.

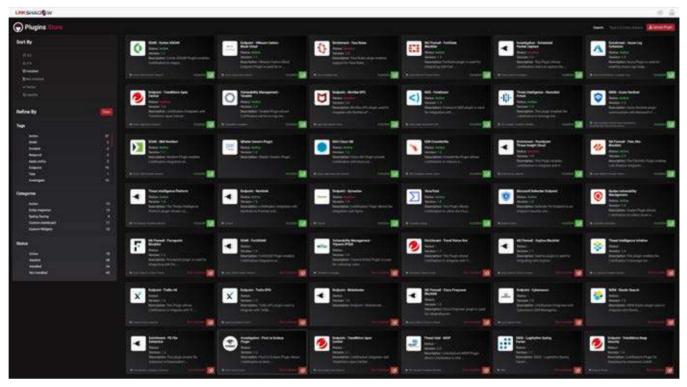
LinkShadow's commitment to security is unwavering, and it places paramount emphasis on customer input. As an AI-

LINKSHADOW PLANS TO INNOVATE AND INVEST CONTINUOUSLY IN R & D.

focused company initially specialising in machine learning models, LinkShadow set out with a clear vision: to fortify organisations against advanced cyber threats, including zero-day malware and ransomware, all while offering rapid insights into the competence of their existing security investments. Over time, it evolved to provide cuttingedge Network Detection and Response solutions. In today's swiftly evolving threat landscape, where innovative cybersecurity approaches are imperative, LinkShadow stands out as a beacon of change.

Patrick Ramseyer, VP, EMEA at

LinkShadow, underscores the company's commitment to its customers and to the broader cybersecurity landscape. He emphasises continued focus on their global expansion strategy, with key upcoming distribution agreements set for the Far East, Africa, and Europe. "The focus remains on continuous growth, achieved primarily through a channelcentric approach. LinkShadow aims to collaborate closely with distributors, system integrators, and managed



security service providers (MSSPs). This indirect sales model aligns seamlessly with our go-to-market strategy," he adds.

In addition to expanding their reach, LinkShadow remains committed to enhancing its product offerings. The company intends to introduce new features that will further distinguish their solutions in the cybersecurity space. With an unyielding commitment to cybersecurity excellence, LinkShadow takes every step necessary to adapt to the ever-evolving threat landscape and ensure their customers have the tools and resources to strengthen their defenses against advanced cyber threats.

The Power of Many

LinkShadow recognises that no organisation can stand alone against the vast array of cyber threats. It actively collaborates with a diverse partner ecosystem and this approach ensures that its solutions are seamlessly integrated into an organisation's existing security infrastructure.

By working closely with its partners, LinkShadow extends its reach and helps organisations of all sizes access cutting-edge cybersecurity solutions. This inclusivity is essential in a world where cyber threats spare no one. Whether a small business or a global enterprise, LinkShadow's partner ecosystem ensures that everyone can benefit from robust cybersecurity measures.

By forging strong relationships with these vendors, LinkShadow leverages its expertise and technologies to enhance its own offerings. Through integration with best-of-breed security products, LinkShadow creates a synergistic approach to cybersecurity and this allows organisations to benefit from a unified and layered defense strategy.

In Patrick's words: "Collaboration is the way to stay ahead of a complex attack landscape. If you want to stop cyber criminals, if you want to stop anything bad happening, then the best way to do this is to get together. That's our philosophy, that's how we stay ahead of the curve. We leverage the best technology out there via our AI and ML capabilities. We integrate with all the top vendors in the cybersecurity market and all the top threat intelligence feeds. This creates a situation of one plus one plus one is five, because we combine the strength of all of these vendors in the market, that places us in a much more powerful position. The key to defeating cyber threats is alliances."

LinkShadow's commitment to forging strategic alliances with its partner ecosystem and leading vendors demonstrates its dedication to combating the intricate cybersecurity threat landscape. Through these collaborations, LinkShadow strengthens its ability to provide organisations with comprehensive, innovative, and adaptive cybersecurity solutions, ultimately helping them stay ahead of the evolving threat landscape and safequard their critical assets. In an era where cybersecurity challenges continue to evolve, LinkShadow's collaborative approach stands as a symbol of resilience and adaptability.

A Different Take

The traditional siloed approach to cybersecurity relies on expecting a multitude of specialised teams and experts to safeguard an organisation's digital assets. In this model, a large organisation typically maintains a Security Operations Center (SOC) comprised of various teams, each dedicated to specific security functions such as firewall management, endpoint detection and response (EDR), intrusion detection, and data loss prevention (DLP). However, the reality is that there is a shortage of qualified cybersecurity professionals globally, and the expertise required to excel in these roles demands a steep learning curve.

Moving from a tier one analyst to a tier three analyst involves a significant accumulation of experience and knowledge to effectively combat evolving cyber threats. This fundamental challenge is magnified by the siloed architecture, as it demands a specialist for each security area, which further exacerbates the scarcity of qualified professionals. The result is that organisations lack comprehensive visibility across their entire security landscape.

Consider this scenario: when an organisation attempts to consolidate reports from each specialised team, it can take a week or more to compile and analyse the data. In the fast-paced realm of cybersecurity, a week is an eternity, and the consequences of a cyberattack can be devastating in that timeframe. Moreover, the siloed approach can lead to gaps in threat detection and response. For example, one team may detect suspicious activity in the endpoint realm (EDR), while another remains unaware of the threat in the firewall domain. Savvy hackers can exploit these gaps to infiltrate an organisation's defenses undetected.

This is where LinkShadow takes

LINKSHADOW'S APPROACH ENSURES THAT ORGANISATIONS → NO LONGER HAVE TO STRUGGLE WITH THE CHALLENGES POSED BY THE SILOED MODEL.

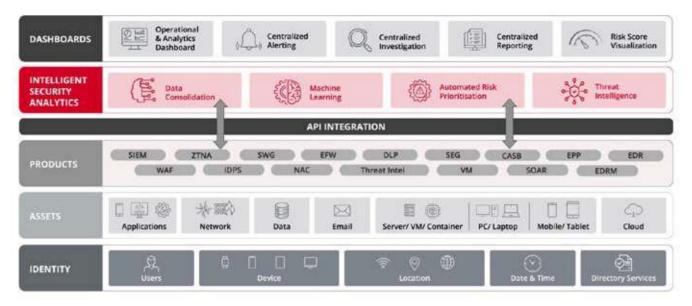


a different route. It recognises that the siloed approach is no longer sustainable in today's rapidly evolving threat environment. Instead of expecting organisations to rely on an ever-expanding pool of specialised experts, LinkShadow's Cyber Mesh platform offers a unified platform that eliminates the need for silos. By providing a comprehensive view of an organisation's security posture and streamlining the monitoring of network traffic, LinkShadow enables proactive threat detection and response, bridging the gaps left by traditional, fragmented security architectures.

In essence, LinkShadow's approach ensures that organisations no longer have to struggle with the challenges posed by the siloed model. With LinkShadow, they can gain comprehensive visibility, consolidate reports efficiently, and respond swiftly to emerging threats. In a world where time and expertise are of the essence, LinkShadow's unified platform represents a monumental shift towards a more effective and efficient security paradigm.

Intelligent Security

LinkShadow's intelligent approach to security makes it a frontrunner in providing cutting-edge cybersecurity solutions. Take the case of its Network Detection and Response (NDR) solution, for instance. "Traditional NDR monitors network traffic in a 'North-South' direction, from outside to inside the network, plus a lateral East-West direction," Patrick says. "Traffic within the network is monitored by connecting to the core switch, the "Span Port." When this switch is connected, it gives a duplicate of all the traffic within the network, which allows IT teams to detect anomalies. LinkShadow's Intelligent NDR, on the other hand, is powered by AI and gives you a lot more. It actually provides Risk Exposure, which allows you to consolidate threats from all your cybersecurity tools and give you a clear



view about where you're most exposed and where your biggest risk is."

"One of the things that LinkShadow does very powerfully, is look at each device and user on a network and consider all the possible, associated risks. For example, on a computer, if the end point detection and response throws up suspicious files, if there are vulnerabilities within the OS, the security patches are not up-to-date, or if there is suspicious traffic. we'll consolidate of all this information, put it all together real-time, and give you the complete picture. In other words, we help reduce 'alert fatigue', a very real problem that security analysts and IT teams face every day. In the traditional security architecture, there is no way of knowing which alert is important. Using our Threat Score Quadrant, we prioritise the many alerts and put forward only what's really needed. We consolidate all the data sources and tell businesses where

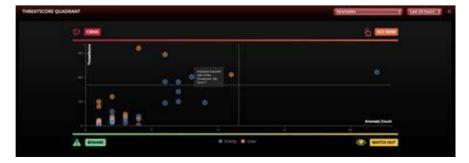
they really need to focus. Ask any SOC manager and they'll tell you that alert fatigue or 'noise' is one of their biggest problems. There are so many systems sending out alerts at the same time, that it becomes extremely challenging to differentiate one from the other. At LinkShadow, we help reduce this noise," he adds.

LinkShadow Cyber Mesh Platform

LinkShadow's Cyber Mesh Platform represents a modern and comprehensive approach to cybersecurity. Some of the advantages of this platform include:

Integration and Consolidation: Cyber

Mesh integrates and consolidates security measures throughout the entire network. This ensures that security is not just an afterthought but is woven into the fabric of the network. This integration helps in closing potential gaps that might exist in a traditional siloed approach.



Better Visibility and Control: With a unified security platform, organizations can have a holistic view of their network. This enables them to identify vulnerabilities and threats more effectively, making it easier to respond to potential risks promptly.

Dynamic and Adaptive Defense: In

a rapidly evolving threat landscape, adaptability is crucial. The cyber mesh architecture allows organisations to respond quickly to emerging threats. It ensures that security measures can be adjusted in real-time, helping in proactive threat mitigation.

Simplification and Reduced Complexity:

Managing multiple disparate security components can be challenging and time-consuming. By consolidating security into a cyber mesh platform, organisations can simplify their security operations, reducing complexity and the resources required for maintenance.

Zero-Trust Approach: The adoption of a zero-trust approach is a significant advantage. Treating every user, device, and application as potentially untrusted means that strict access controls and authentication mechanisms are enforced. This helps in minimising the risk of unauthorized access and internal threats, which are increasingly common in today's threat landscape.

In summary, the Cyber Mesh Security Architecture, exemplified by the LinkShadow Cyber Mesh Platform, offers a complete and forward-looking approach to cybersecurity. It addresses the limitations of traditional, siloed security measures by integrating security throughout the network, promoting adaptability, simplifying management, and emphasising a zerotrust model to enhance overall security posture. It's important for organisations to carefully consider such architectural approaches to stay ahead of evolving cybersecurity threats.

Technology Integration

With LinkShadow, technology integration is seamless and easy. The CSMA-Approach offers a dynamic and proactive approach to cybersecurity that empowers IT teams to integrate various technologies and provide enhanced visibility, agility, and a strong overall security posture.

LinkShadow already integrates with over 60 vendors and has a full team of developers dedicated to just system integrations, in Dubai alone. This means that whatever security tool a customer has, LinkShadow can integrate all of that within 15 working days, provided there's an open API. And this integration will be available to every other customer in the future. Moreover, it is built in such a way that the integration can be easily downloaded, just like an App, all plug and play. If a customer wishes to integrate an EDR, for instance, he can just download it and like any other app, it will install on his system and he will be guided step-by step on how to configure his EDR and his LinkShadow solution, so that they talk to each other.

"Our technology integration is as easy as an app. So, if a cybersecurity customer wishes to buy a new security tool, the likelihood is that it is already on LinkShadow, and if it's not, we'll integrate it for you. This is key to the Cybersecurity Mesh Architecture approach -the ability to integrate with other technologies."

The Real Benefit

In today's cybersecurity landscape, the boardroom is increasingly focused on understanding the strength of an organisation's security posture. It's not enough to simply have robust cybersecurity measures; businesses must also be able to generate comprehensive boardroom reports that convey how well-protected the organisation is. This involves showcasing the ability to consolidate and mitigate risks effectively. This is where LinkShadow helps enhance efficiency and streamline security operations.

"When it comes to investment decisions, decision-makers primarily consider two key factors: How will this benefit the organisation by reducing risk, and how will it impact the budget? It's crucial to demonstrate cost savings and operational efficiency improvements. LinkShadow achieves this by streamlining security operations. We optimise Security Operations Centers (SOCs) to enhance efficiency and reduce the need for excessive staff. This is achieved through automation and intelligent integration. One compelling example of our capabilities involves automating the integration of threat intelligence feed, saving a client an impressive two-and-a-half hours daily. This translates to 15 hours per week, equivalent to half a staff member's workload. Such integration and automation are pivotal in cost-saving strategies."

Automation is the lynchpin for financial prudence in cybersecurity. Organisations looking to make investment decisions should prioritise automation to reduce manual tasks, enhance their risk posture, and improve SOC efficiency.

Board members and CFOs require tangible evidence of the value brought to the business. They need to see a reduction in risk exposure as a direct result of adopting LinkShadow's solutions. This is especially critical when considering the average cost of a cybersecurity breach, which hovers around three and a half million dollars. In some cases, breaches can cost hundreds of millions due to extensive recovery efforts. The core of an investment decision lies in mitigating such potential financial losses.

To further understand LinkShadow's unique features and capabilities, we need to examine the metrics that matter to SOC managers. These metrics include mean time to detection, mean time to response, mean time to investigation, and dwell time. LinkShadow significantly improves these metrics by automating processes, correlating data, and leveraging Al and machine learning to enhance the efficiency of SOC operations.

For instance, in the case of a malware threat resulting from a phishing email, LinkShadow's unified approach detects anomalies across multiple security tools. It brings together insights from EDR, email gateways, firewall reports, and other sources, providing a comprehensive view that significantly reduces the chances of oversight. This is a core aspect of SOC efficiency that has contributed to LinkShadow's strong reputation in the cybersecurity industry.

LinkShadow's ability to automate, integrate, and enhance SOC operations translates into tangible benefits for organisations, including reduced risk exposure, cost savings, and improved efficiency. These are the critical factors that guide investment decisions in today's cybersecurity landscape.

Staying Ahead

LinkShadow plans to innovate and invest continuously in R &D. At the heart of LinkShadow's success story lies its pioneering approach to harnessing the

LINKSHADOW'S ABILITY TO AUTOMATE, INTEGRATE, \rightarrow AND ENHANCE SOC OPERATIONS TRANSLATES INTO TANGIBLE BENEFITS FOR ORGANISATIONS.



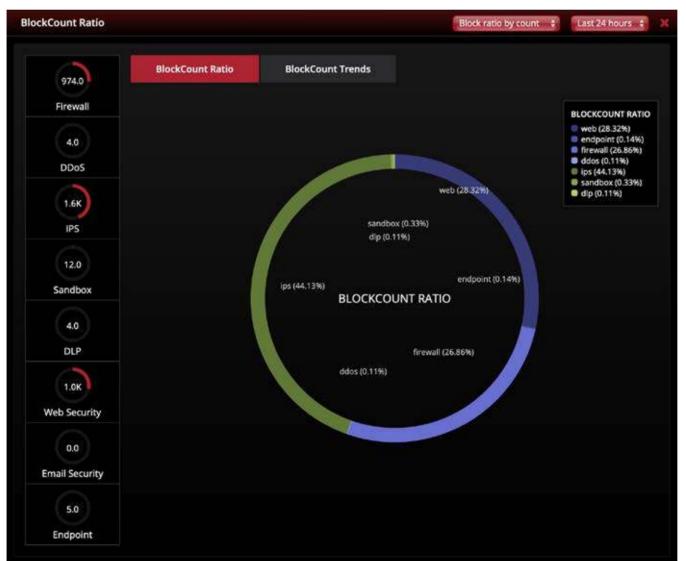
power of Artificial Intelligence (AI) in cybersecurity. While AI is often touted as a buzzword in the industry, LinkShadow recognised its true potential long before it became a ubiquitous term. The company's early realisation that AI's true strength lies in its ability to correlate and consolidate data from multiple sources set it on a path of continuous innovation.

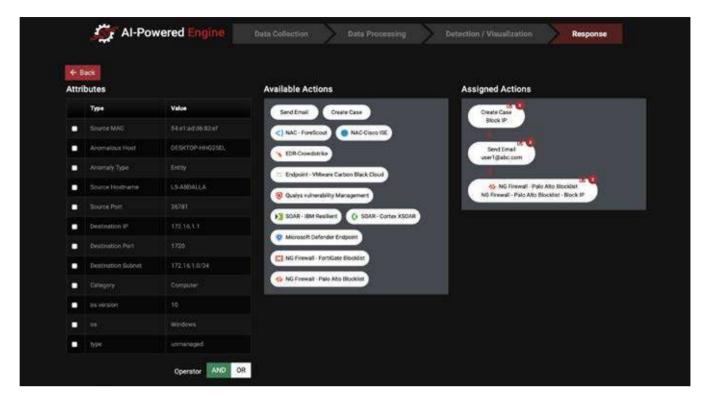
"LinkShadow recognised early on that AI's greatest strength lies in its ability to correlate and consolidate data from multiple sources, providing a comprehensive overview of the cybersecurity environment. In the cybersecurity sector, we were discussing AI long before it became a buzzword or marketing gimmick. While some competitors also leverage AI effectively,

LINKSHADOW RECOGNISED EARLY ON THAT AI'S GREATEST STRENGTH LIES IN ITS ABILITY \rightarrow TO CORRELATE AND CONSOLIDATE DATA FROM MULTIPLE SOURCES.

we consider ourselves modern innovators within the industry. Our journey started with this realization and has since evolved. We've expanded our presence into various markets, including the Middle East, Asia, and Europe. Notably, we've gained the trust of major government and financial institutions, affirming the acceptance of our technology and our market positioning. Our approach has shifted from merely showcasing product features to addressing the broader business concerns of our customers. These concerns span financial, staffing, and security issues. This approach has resonated well with our customers and enhanced our reputation as a transparent company that offers a robust cybersecurity solution.

At LinkShadow, we believe in collaboration rather than claiming superiority over others. We focus on





synergy, where one plus one equals five. Personally, I'm convinced that LinkShadow is poised to become a global leader in this market due to its exceptional technology and approach.

To maintain our position at the forefront of the industry, we have a comprehensive roadmap in place. This encompasses AI advancements and numerous integrations. Our commitment to continuous innovation and substantial investment in research and development ensures that we stay ahead of the curve. Listening to our customers and sales teams remains paramount. Our approach is to understand their cybersecurity challenges and tailor solutions accordingly. In essence, our communication strategy revolves around three key words: listen, listen, listen. This

LINKSHADOW CYBER MESH PLATFORM, OFFERS A COMPLETE AND FORWARD-LOOKING APPROACH TO CYBERSECURITY. approach will keep us at the forefront of cybersecurity for years to come."

LinkShadow's innovative use of AI and machine learning has redefined the way organisations approach cybersecurity. It goes beyond marketing gimmicks and empty promises; LinkShadow integrates AI seamlessly into its solutions, enhancing threat detection, response, and investigation capabilities. This deep integration has allowed organisations to stay ahead of emerging threats, outsmart cybercriminals, and safeguard their digital assets effectively.

LinkShadow's journey is marked by significant milestones in the cybersecurity landscape. From its inception, the company demonstrated a remarkable vision, expanding its reach into various markets around the world. But what truly sets LinkShadow apart is its uncompromising stance on eliminating even the most complex of threats. In an era where cyberattacks have grown in sophistication, LinkShadow's solutions stand as a fortress against these evolving dangers. The company's dedication to bolstering security operations centers (SOCs) has resulted in remarkable improvements in critical metrics. Mean Time to Detection, Mean Time to Response, Mean Time to Investigation, and Dwell Time have all been significantly reduced, thanks to LinkShadow's intelligent automation and data correlation capabilities.

LinkShadow is not just a cybersecurity product vendor; it's a visionary trailblazer that has reshaped the industry's landscape. Its journey from recognising AI's potential to becoming a global leader is a testament to its dedication and commitment. The milestones it has achieved, combined with its unwavering focus on innovation and security, make it a formidable ally for organisations looking to protect their digital assets in an increasingly perilous cyber world.

In an age where threats constantly evolve and cybersecurity challenges grow in complexity, LinkShadow remains steadfast in its mission to safeguard organisations, and we can only anticipate greater innovations and achievements from this industry leader in the years to come. As the digital realm continues to expand, LinkShadow stands as a resolute guardian, ensuring that organisations can thrive in a secure and resilient cyber environment.

Digital Transformation Simplified

CITUS abs Your Journey Is Our Journey

	PILLARS	BLOCKS	OUTCOMES
	Agile Product Management	Design Thinking Innovation Ecosystem Product Portfolio	Competitive Advantage
	Artificial Intelligence	NLP Predictive ML Generative Al Ops XReality Robotics Computer Vision	Disruptive Innovation
	Data	Data Strategy Data Integration Data Warehouse Data Governance Data Quality	Predictive Analytics
\bigcirc	Security	Governance Risk Compliance Cyber Security Monitoring	Compliance & Governance
0	Cloud Computing	Cloud Strategy Application Development Cost Optimization Call Center	Secure Scaling
*	Modernized Technology	Architecture Software Delivery Testing DevSecOps API Hub	Future Ready
©,	Agile Organization	Train Launch Coach Scale	Customer-centric Innovation
部	Digital Strategy	Visioning Technology Strategy Policy	Unified Vision

Learn more by scanning the QR Code:



or visit us at: Hall 26 - B25





Hosted by







WORLD'S LARGEST Startup event Just Got Bigger



EXPAND

NORTH

170,000 TRADE BUYERS

6,000+ EXHIBITORS

EXHIBITING

COUNTRIES

1,400+ speakers

900+

INVESTORS

100+

250+ speakers

176

ATTENDING

COUNTRIES



REGISTER NOW FOR FREE

1.800+

STARTUPS

GLOBAL

COMPREHENSIVE SECURITY

hat are some of the recent, key milestones attained by NetWitness? In order to truly

appreciate the milestones we've achieved in the past year, it's essential to delve into the history of RSA and NetWitness. NetWitness has been a part of RSA for the past 12 years. However, when STG decided to acquire RSA, they made the strategic decision to spin off all the business units. Two years ago, we began our journey as a standalone company. Perhaps the most significant milestone we reached last year was appointing our own CEO, highlighting the paramount importance of our company's evolution and expansion. For guite some time, we've maintained a laser-focused strategy aimed at expanding our technology and presence in the market, guided by a clear roadmap and a five-year vision for our technology.

ABDULLAH ALSAADOUN,

DIRECTOR META, AT NETWITNESS, TELLS ANITA JOSEPH ALL ABOUT THE COMPANY AND ITS COMPREHENSIVE, END-TO-END VISIBILITY PLATFORM THAT COMES EQUIPPED WITH DIVERSE SECURITY CAPABILITIES.





NetWitness will attend GITEX Global & Black Hat MEA. Why are these events important, and what are your goals? Participating in GITEX and Black Hat is integral to our global marketing and branding strategy. We've meticulously crafted our marketing plan for this year and the next to ensure comprehensive coverage across the Middle East, Turkey, and Africa region. GITEX and Black Hat occupy the top positions on our list. These events are truly global in nature, attracting key decisionmakers, government entities, and enterprises from around the world. Our presence at these two crucial events serves to reassure our markets that we are committed to robust growth and expansion.

What is the USP of the NetWitness Threat Detection & Response platform, and why is it called an Open Platform?

Our unique selling proposition lies in the fact that we offer an end-toend visibility platform that remains unparalleled in the market. We cover every facet of SOC (Security Operations Center) operations, commencing with log management using the same technology. This extends to NDR (Network Detection and Response), Endpoint Detection and Response, all powered by machine learning in UEBA (User and Entity Behavior Analytics), and complemented by SOAR (Security Orchestration, Automation, and Response) technology. Furthermore, all these capabilities seamlessly integrate with the Incident Response (IR) services that NetWitness provides. It's worth emphasising that no other company in the world presently offers such a comprehensive platform with such diverse capabilities. This platform simplifies SOC operations and provides analysts with a unified, single-pane-of-glass technology, significantly enhancing their effectiveness. 1



Secure Your Digital Future Simple. Secure. Resilient.

0

0

0

17

Secure Your Enterprise IT Footprint For A Safer Digital Journey

> www.raqmiyat.com UAE | KSA | INDIA



THE NEXT 50 YEARS: SHAPING A SECURE WORLD

ANITA JOSEPH MET WITH **DR. MOHAMMED AL-KUWAITI**, HEAD OF THE UAE CYBERSECURITY COUNCIL, TO FIND OUT MORE ABOUT WHAT THE FUTURE HOLDS FOR THE UAE IN TERMS OF TECHNOLOGY AND DIGITAL GROWTH.

uman resource is our biggest strength. As we move forward in the technology-powered world, we will continue to invest in people, equipping them with the necessary skills to take on a digital tomorrow and ensure safety of digital assets," said Dr. Mohammed Al-Kuwaiti, Head of the UAE Cybersecurity Council, speaking exclusively to Tahawultech.com

He was participating in the "Cyber Next 50: Securing the UAE's 2071 vision", a joint media event by the UAE Cybersecurity Council in collaboration with KPMG Lower Gulf, on an upcoming joint report highlighting major trends expected to impact life in the coming decades.

"The UAE today is a global hub of dynamism, with a happy and harmonious society. It has been a privilege to witness the UAE's rapid transformation over the years, and we look forward to its continued advancement in digital and cyber innovation. As the UAE looks forward to its Centennial in 2071, we had an opportunity to pause, examine how the world might evolve over the coming decades, and how we can leverage technology to optimise outcomes for humanity," Dr. Mohammed said.

He added, "The UAE stands as a dynamic global hub, characterised by a harmonious and contented society. Witnessing the UAE's remarkable transformation has been a privilege, and we eagerly anticipate its continued progress in digital and cyber innovation. As we approach the UAE's Centennial in 2071, we have taken this opportunity to pause and contemplate the future's evolution and how technology can optimise outcomes for humanity. We all know that the seeds of tomorrow are sown today and that we have an extraordinary chance to shape a safer world for future generations. We eagerly look forward to taking the nation on a path of unprecedented growth and technological advancement in the next five decades and beyond."

The upcoming report, set to be unveiled soon, casts a spotlight on megatrends poised to impact life in the approaching decades, encompassing demographic shifts, climate change, and burgeoning energy consumption. With a projected global population of 9.7 billion by 2050, diverse societal risks loom over various regions. Climate change exacerbates food security challenges, contributes to population displacement, and precipitates ecosystem degradation. As global energy consumption is slated to surge by 50% by 2050, the importance of renewable energy sources and enhanced energy efficiency is more pressing than ever.

Dr. Mohamed Al Kuwaiti emphasised that these challenges mandate concerted efforts to confront and mitigate their repercussions. Simultaneously, he underscored hope that technology represents for a brighter future. Anticipated technological advancements encompass artificial intelligence, hyper-connectivity, bioengineering, quantum computing, space technology, robotics, smart manufacturing, augmented reality, and nuclear fusion.

The report anticipates a future where immersive virtual reality blurs the lines

between reality and fiction, businesses thrive in the virtual realm, and data assumes the role of currency. Robots seamlessly integrate into our daily lives, spanning personal care to military applications, while AI evolves to predict and shape the future. Machines may even gain the capacity to decipher human thoughts and manipulate DNA.

KPMG experts meticulously examined contemporary social, economic, and political trends alongside emerging information technology trends. They synthesised these insights into a series of "Imagine if" scenarios, exploring the potential socio-political ramifications of technological leaps. These scenarios encompass themes like virtual worlds, robotics, and AI.

The report envisages a future where integrity takes center stage, ushering in transparent supply chains and elevating cybersecurity as an indispensable facet of national defense. The definition of humanitarian aid may evolve to encompass 'cybersecurity aid' as cyberattacks increasingly imperil vulnerable populations with limited resources.

By 2071, the quality of life and happiness will be intricately linked to a secure and seamless hybrid of the physical and digital realms, where citizens can freely engage, work, and revel in their pursuits. Already acclaimed as the happiest place to reside in the Arab world, according to the latest UN World Happiness Report 2023, the UAE must adapt its cybersecurity legislation to navigate the challenges of the next five decades effectively.

THE NEW CISCO SECURE APPLICATION OFFERING GIVES CUSTOMERS EXPANDED VISIBILITY AND INTELLIGENT BUSINESS RISK INSIGHTS ACROSS CLOUD ENVIRONMENTS.

CISCO SECURE APPLICATION DELIVERS BUSINESS RISK OBSERVABILITY FOR CLOUD NATIVE APPLICATIONS

isco has announced the availability of Cisco Secure Application (previously Security Insights for Cloud Native Application Observability) on the Cisco Full-Stack Observability Platform, enabling organisations to bring together application and security teams to securely develop and deploy modern applications. The latest release of Cisco Secure Application helps customers to securely manage cloud native applications in addition to hybrid applications.

In the race to deliver seamless digital experiences, IT teams have experienced an increase in the need to shift to modern, distributed applications, but according to a recent Cisco study, 92% of global technologists admit that the rush to rapidly innovate and respond to the changing needs of customers has come at the expense of robust application security during software development.

This has left companies exposed to security vulnerabilities and threats, with larger attack surfaces and gaps in their application security layer caused by siloed teams both struggling to gain visibility and the right business context to prioritise vulnerabilities. As a result, organisations are reporting an explosion of security incidents in the modern environment, putting customer data and the reputation of their business at risk.

To help organisations secure cloud native applications, the new Cisco Secure Application offering — now available on Cisco's recently launched Full-Stack Observability Platform — arms customers with expanded visibility and intelligent business risk insights across cloud environments, empowering businesses to better prioritise and respond in real-time to revenue and reputation-impacting security risks and reduce overall organisational risk profiles.

Cisco Secure Application integrates with Cisco's industry leading security products and enables customers to:

- Locate and highlight security issues across application entities, including services, workloads, pods, containers and business transactions, and isolate them at speed.
- Prioritise issues with a business risk score that combines application performance data and business impact context from Cisco's own Cloud Native Application Observability, with real-time vulnerability detection and security intelligence from Cisco's security products, to identify which business transactions present the greatest risk.
- Accelerate response time to security incidents with real-time remediation guidance, complete with prescriptive actions to prioritise and address the most impactful security vulnerabilities.

"Application security has never been a more pressing priority for businesses, and traditional vulnerability scanning solutions simply don't provide the information that teams need," said Ronak Desai, Senior Vice President and General Manager, Cisco Full-Stack Observability

and AppDynamics. "An organisation's ability to quickly assess risks based on potential business impact, align teams and triage threats is entirely dependent on understanding where vulnerabilities exist, the severity of those risks, the likelihood they will be exploited, and the risk to the business of each issue. This business risk observability can help IT professionals understand and prioritise those risks and is uniquely delivered by Cisco. The availability of Cisco Secure Application on the Cisco Full-Stack Observability Platform is a critical next step in our commitment to providing customers with the tools they need to deliver unmatched and secure digital experiences across hybrid and multicloud environments."

"The successful digital infrastructure must operate as a concert — not as a collection of separate products, providers, and people. This requires all components — from core to edge, from network to applications, from on-premises systems to public cloud and communications services — to work as one to deliver the best digital experiences," said Mark Leary, Research Director, IDC. "Cisco's extensive domain experience across hybrid and multi-cloud environments and comprehensive full tech stack oversight positions the company well to help customers bring application observability, security intelligence data, and business risk observability together. Combined, they give customers access to the critical information they need to make smart decisions about their application security," he added. 🙎

POWERED RVAI

TATE WU, GENERAL MANAGER OF HIKVISION UAE, OMAN & YEMEN, TELLS SECURITY ADVISOR ABOUT THE COMPANY'S PARTICIPATION AT GITEX, THE GROWTH OF AI AND PLANS FOR THE REGIONAL MARKET.

an you tell our viewers about some of the products, solutions, and partnerships that you have announced at GITEX 2023?

This year, our national distribution partners in the UAE represent us at GITEX, where visitors can immerse themselves in Hikvision technology. Visitors can experience various product ranges, such as cutting-edge CCTV products and intelligent solutions.

Hikvision has been demonstrating its versatile AI solutions at GITEX in the past few years. This year together with our partners, we will focus on Hikvision intelligent vertical solutions across industries such as education, energy, logistics, retail, smart city, and smart homes. Our national distributors will show visitors how Hikvision's AI technologies and solutions can help customers and create value for them.

We know that technology is growing at rapid speed, and the IT ecosystem is constantly evolving. However, what trends and technologies do you see driving new innovations in 2024 and beyond?

The top 3 trends for technologies in 2024 in my opinion will be, first of all Al. Nowadays, Artificial Intelligence is quite common in the security industry. More customers in the industry have recognised the value of Al, and have found new uses for Al applications in various scenarios, along with ANPR, automated event alerts, and false alarm reduction and much more. Al has been



AIOT BRINGS MORE POSSIBILITIES TO THE INDUSTRY WITH APPIDLY EXPANDING APPLICATIONS FOR SECURITY DEVICES AND SYSTEMS.

one of the fundamental technologies to reshape the security industry.

AloT will digitise and pervade industry verticals, from our perspective, AloT brings more possibilities to the industry with rapidly expanding applications for security devices and systems. Green manufacturing and low-carbon initiatives are valued by societies around the world and will also take big strides. In the security market, we have seen products featuring low-powerconsumption become the preferred options for customers, and demands for solar-powered cameras are increasing.

What is Hikvision's plan for the regional market in the coming years?

For the region, we have divided our business into channel and project business segments. In the channel, we are well established and we strive to provide an effective one-stop-shop solution for all partners, so that they from the full Hikvision product line offerings. For the project business, we can see that the trends dominating the market right now are digitalisation and AI and that the demand for hosted solutions and IoT are also ramping up. So, we plan to provide vertical solutions in these areas to our end users to allow them to operate in a safer environment and also to increase their operational efficiency and reduce costs, so as to make their businesses more profitable. So that's going to be our strategy and focus for the region. 1

SMARTER AND SAFER

ANITA JOSEPH CAUGHT UP WITH **MOHAMMAD MERAJ HODA,** VICE PRESIDENT – EMERGING MARKETS AT RING, TO DISCUSS HOW THE COMPANY CONTRIBUTES TO A SMARTER AND SAFER COMMUNITIES.



ill Ring be present at GITEX 2023? If so, what are you showcasing at the event?

Yes, we will be participating at GITEX 2023. We will exhibit our entire product line-up highlighting our whole-home security solutions, from Video Doorbells, indoor and outdoor Security Cameras to Ring Alarm. We are looking forward to insightful discussions on how smart security devices can help keep customers connected to their homes for added peace of mind and convenience.

Stronger communities are the key to safer neighborhoods. Give us an overview of some of Ring's latest, cutting-edge products that contribute to a safe community.

We are committed to delivering wholehome smart security solutions that are convenient and easy to install for families, and we're excited to demonstrate our newest innovations at GITEX 2023.

Ring's latest smart security offering in the Middle East is Indoor Camera (2nd Gen), our first-ever security camera with a manual Privacy Cover, that disables audio and video recording when placed over the camera lens. Now, customers can have even greater control over what their device captures for increased privacy.

Our new Battery Video Doorbell Plus, which was also launched this summer, is the first battery-powered doorbell in our line-up with 1536p HD video and a headto-toe field of view which makes features like Package Alerts even more helpful.

Additionally, we released Spotlight Cam Plus earlier this year, a versatile outdoor camera with a dual-power option, Color Night Vision, and motionactivated LED lights. This provides homeowners with clear visuals of their property during the day and at night.

All our devices can be linked and managed from the free Ring app, providing users with real-time access and control over their home security, no matter where they are.



Can you elaborate on how Ring uses cloud technology for data storage in its devices?

All of the events captured by your Ring device are recorded and stored in the cloud for up to 180 days with an optional Ring Protect subscription plan. You can easily scroll through your timeline to check out what moments you missed throughout the day. You can also download your videos to save them for later and even share them with friends, family and neighbours. Without a Ring Protect Plan, you'll still receive real-time notifications when motion is detected and can check in on the Live View of your devices from the Ring app, but you won't get video recordings of those events.

How can office spaces benefit from implementing Ring's smart security solutions?

While we design our devices with residential use in mind, we have heard from customers who have placed Ring Alarm systems in their small businesses for an added layer of security and peace of mind. When Ring Alarm's sensors detect motion, the siren is triggered and the customer will receive a realtime motion alert to their Ring app. The Ring app also allows customers to arm and disarm their Ring Alarm remotely and tailor the system to their needs, for example by setting schedules for when the alarm should be armed or disarmed, during working hours vs. after hours.

What are your plans for the Middle East market going forward?

At Ring, we're focused on customer feedback and innovating on our customers behalf to meet regional needs and preferences and give customers the tools they want, to build out their home security systems and make their day to day lives more convenient and secure. For example, we recently incorporated advanced radar-powered features into our pro outdoor camera range to give our customers more control over their motion alerts and context surrounding their motion events.

ALL OUR DEVICES CAN BE LINKED AND MANAGED FROM THE FREE RING APP, PROVIDING USERS WITH REAL-TIME ACCESS AND CONTROL OVER THEIR HOME SECURITY, NO MATTER WHERE THEY ARE.

ACTIVE DIRECTORY AND SECURITY

ANITA JOSEPH CAUGHT UP WITH **JOHN SHIER**, FIELD CTO AT SOPHOS, TO DISCUSS THE IMPORTANCE OF ACTIVE DIRECTORY AND THE FINDINGS OF THE ACTIVE ADVERSARY REPORT FOR TECH LEADERS 2023.

ell us more about the findings of the Active Adversary Report for Tech Leaders 2023

Cyberattacks aren't slowing down. Ransomware is still the most prevalent type of attack in the Incident Response cases handled in the first half of 2023. Ransomware accounted for 69% of the cases Sophos investigated. Sophos X-Ops found that median attacker dwell time — the time from when an attack starts to when it's detected decreased from 10 to eight days for all attacks, and from nine days to five days for ransomware attacks. In addition, it took on average less than a day approximately 16 hours — for attackers to reach Active Directory (AD), one of the most critical assets for a company.

Why is Active Directory (AD) so critical for an organisation?

Attacking an organisation's Active Directory (AD) infrastructure makes sense from an offensive view. AD is usually the most powerful and privileged system in the network. AD typically manages identity and access to resources across an organisation, meaning attackers can use AD to easily escalate their privileges on a network to simply log in and carry out a wide range of malicious activities across multiple systems. Beyond providing broad access to the systems, applications, resources and data that attackers can exploit in their attacks, AD can also be used to launch attacks through



domain-wide policy changes. When an attacker controls AD, they can control the organisation. The impact, escalation, and recovery overhead of an Active Directory attack is why it's targeted.

The Report states that Dwell Time— Time from the Start of an Attack to When It's Detected—Shrinks to 8 Days. Does this mean we've become more secure as a result of our collective efforts?

The reduction in dwell time reflects actions on both sides of the attack equation. The proliferation of modern cybersecurity technologies has increased our visibility to attacks. This improved visibility has lowered the mean time to detect (MTTD) of attacks and allows organisations to initiate response sooner. This has meant that attackers have been forced to accelerate. Many criminals now know that they have to move quickly before

THE IMPACT, ESCALATION AND RECOVERY OVERHEAD OF AN ACTIVE DIRECTORY ATTACK IS WHY IT'S TARGETED.

they are detected and are therefore more focused on their objective. We've seen some ransomware gangs switch to data extortion without encryption, which is much less noisy, possibly as a response to this new detection environment. Finally, some professional cybercrime gangs have had so much practice running through their attack playbooks that they've likely found ways to operate more quickly and efficiently.

Will Sophos be a part of GITEX 2023? What will be the main focus of your participation?

Yes, this is our fourteenth year at GITEX Global and we will showcase our latest cybersecurity innovations and services including Sophos Managed Detection and Response (MDR) and Sophos Incident Response services that can help organisations achieve optimal cybersecurity results by implementing an effective cybersecurity strategy. Additionally, we will focus on our complete, integrated, cybersecurity as a service platform and introduce Sophos Incident Response Retainer, which provides organisations with speedy access to Sophos' industry-first fixed-cost incident response services that includes 45 days of 24/7 Managed Detection and Response (MDR). 1

INTERVIEW / GENETEC

MAKING IT EASIER TO PROTECT THE EVERYDAY

ON THE SIDELINES OF INTERSEC SAUDI ARABIA 2023, **FIRAS JADALLA,** REGIONAL DIRECTOR AT GENETEC, HIGHLIGHTS HOW SECURITY PROFESSIONALS CAN REMAIN AGILE IN ADOPTING NEW APPROACHES AND TOOLS AS DIGITALISATION SWEEPS THE KINGDOM.

o begin with, how have you witnessed the physical security landscape evolve in KSA this year?

It's clear that enhanced security infrastructure is essential to a vision for modernised urban living and a diversified economy. These are driving forces within Saudi Arabia as the country advances towards its Vision 2030 goals. The momentum behind smart city development in KSA has only accelerated this year. You see this in cities such as Riyadh, Makkah, Jeddah, and Madinah, all ranked in the IMD Smart City Index (SCI) list for 2023. When you add projects like Neom and The Line, there's a recognition among both public and private sector leaders that robust physical security solutions for the everyday can provide a more in-depth view of their environmentsenabling organisations to quickly

respond to and recover from any incidents they may face.

What are some of the insights you've discussed with partners at Intersec Saudi Arabia following Genetec's latest State of Physical Security report?

One thing we've been looking at is how labor shortages are driving demand for unified security solutions. For instance, 50% of respondents in that report said their physical security team experienced human resource challenges last year. Today, security leaders are re-evaluating their technology stack seeking solutions that help streamline tasks, automate processes, and enhance team efficiency.

We also see hybrid-cloud deployments driving demand for cloud-connected appliances. Hybrid-cloud deployments are clearly gaining traction. As businesses rationalise costs, concerns, and approach to cloud migration, we can expect an increase in demand for readyto-deploy hybrid-cloud appliances.

Moreover, the research shows us that IT and security professionals are looking to invest in cybersecurity-related tools to improve physical security in 2023. In the Kingdom, a more holistic, automated approach to defending against threats is taking precedence today, as is proactive security architecture planning and procurement.

With cybersecurity being such a critical element to national development plans in KSA today, what is Genetec doing to strengthen and differentiate its own cybersecurity posture in the industry? One of the things that differentiates us is that our cybersecurity posture is built into the fabric of our business. This is not only to protect our own networks but also as a fundamental design principle in the development of our products. Genetec

ONE OF THE THINGS THAT DIFFERENTIATES US IS THAT OUR CYBERSECURITY POSTURE IS BUILT INTO THE FABRIC OF OUR BUSINESS.



has a dedicated cybersecurity and security architecture team focused on tracking cyber issues across the industry. Our dedication to continually reviewing the latest technology developments and related cybersecurity best practices ensures that we stay ahead of potential vulnerabilities, integrate updates into our solutions quickly, and uphold the very highest industry standards and protocol.

Genetec has also placed a lot of emphasis on a "unified" architecture approach. How does that add value to a smart city project or to an individual customer?

Over the years, we've observed how organisations were increasingly challenged by analog and unconnected physical security systems. We also noticed a high level of redundancy with as much as 70% of security functionality common between systems.

In response, we developed the Genetec Security Center, an enterprise security platform designed to unify video surveillance, access control, and automatic license plate recognition functions so they would work as one. This unified platform is a comprehensive software solution that manages the different components of a security environment through a centralised open architecture built to provide complete access to all data.

Importantly, a unified system not only looks like a single system, but preserves the ability to bring on other applications and sensors from other solution providers on to the unified platform. By doing so, unification provides everything security personnel need within a single UI to help them effectively and efficiently protect people and assets. While other companies might also use the word 'unification' as part of their marketing message, no other vendor besides Genetec provides a platform where multiple security products are truly built together as one.

This unified approach is the ideal setup for any smart city project and is already delivering great benefits to our customers locally and abroad.

Genetec also takes a strong stance on privacy. Why do you feel that resonates with your customers locally?

Genetec follows privacy by design methodologies, which means that we develop our products with privacy in mind right from the start. It is our default mode of operation and involves proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices from the first line of code to the third-party vendors selected for partnership and integration. It is a philosophy that customers appreciate in collaborating with us, and again, something that sets us apart in the marketplace.

Whether it is through a unified architecture approach or a strong stance on privacy, I'm very proud of our local Genetec teams who are working every day to ensure people, organisations, and communities in Saudi Arabia and the wider region keep moving safely and securely.

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

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

OFFICIAL DISTRIBUTION

PARTNER

SPIRE

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

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

HOSTED BY

مجلس الأمن السيبراني CYBER SECURITY COUNCIL





OFFICIAL GOVERNMENT



GOLD SPONSOR

CLOUDFLARE

OFFICIALLY SUPPORTED BY



ORGANISED BY









، شرطة دب*ب* DUBAI POLICE

مركز حبتي التجاري العالمتي DUBAI WORLD TRADE CENTRE

SMARTER AND SAFER

ANITA JOSEPH SPOKE TO SUJOY BANERJEE, ASSOCIATE DIRECTOR AT MANAGEENGINE, TO FIND OUT HOW THE COMPANY'S LATEST SECURITY SOLUTIONS HELPS BUSINESSES RESIST NEW AND EMERGING THREATS.

> ell us about ManageEngine's latest security solutions. How do they help businesses guard against new and emerging cyber

threats?

ManageEngine's latest additions to their security suite includes the launch of the MSSP (Managed Service Security Provider) edition of its cloud-hosted SIEM solution, Log360 Cloud. With budgeting constraints, organisations are on the lookout for cost effective solutions since the cost of deploying and managing security solutions has become higher than managed security services.

Hence, more and more organisations are tapping into MSSPs for their security needs. The MSSP edition of Log360 cloud look to address the unique business needs of organisations and help in driving up profits.

ManageEngine also recently announced the launch of Identity360, its cloud-native identity management platform that addresses identity and access management (IAM) complexities within enterprise workforces. Enterprises are now focusing on enabling the mobility of workforces without compromising on their security. Thus, it becomes crucial to handle identity complexity effectively and to ensure regulatory compliance while also prioritising a seamless user experience.

Identity security is becoming increasingly relevant today. Tell us about ManageEngine's approach to identity security

In today's interconnected digital landscape, the significance of identity security has never been more pronounced. As cyber threats become increasingly sophisticated, the traditional perimeter-based security approach is proving to be insufficient. The new frontier in cybersecurity is identity. Recognising this paradigm shift, ManageEngine has positioned itself at the forefront with its specialised solutions.

IAM solutions by ManageEngine that comprises AD360 and Identity360, are not just tools but strategic assets for enterprises. As organisations grapple with a dispersed workforce, remote access, and a myriad of devices connecting to their networks, the importance of ensuring that the right person has the right access has skyrocketed. ManageEngine's IAM solution addresses this by offering a comprehensive suite of features that not only manage user identities but also ensure that access is granted based on real-time risk assessments and contextual data.

Complementing this is ManageEngine's SIEM solution, Log360 which delves deep into the log data to unearth patterns and anomalies. In an era where breaches are becoming commonplace, having a SIEM solution that can provide real-time alerts and insights is invaluable.

The true strength of ManageEngine lies in its understanding of the evolving nature of identity security. As they offer both onpremises and cloud deployment options, they meet the needs of modern enterprises



in terms of flexibility and scalability.

The importance of identity security is increasing in today's digital age, and ManageEngine's proactive and comprehensive approach makes them an ideal ally for enterprises trying to navigate the complex waters of cybersecurity.

Data is the new gold and AI is the new tool. How is ManageEngine incorporating AI into its data security offerings?

In today's digital age, where data is likened to gold, tools like AI have become pivotal in safeguarding this resource. Recognising this, ManageEngine has been at the forefront, incorporating AI into its security line up.

One of the transformative ways AI enhances security is by enabling the shift from static to dynamic thresholds. Traditional models of security work on set parameters, but with AI, these boundaries

THE TRUE STRENGTH OF MANAGEENGINE LIES IN ITS UNDERSTANDING OF THE EVOLVING NATURE OF IDENTITY SECURITY. are ever-evolving. By understanding trends, seasonal variations, and random patterns, Al-driven solutions provide a more robust security net.

Additionally, as cyber attackers leverage sophisticated AI tools, the defense mechanisms should be equally, if not more, AI-powered. ManageEngine understands this evolving threat and designs solutions to combat it effectively.

A significant AI-driven feature is UEBA (User and Entity Behavior Analysis). By continually screening user and entity behavior, it's possible to detect unusual patterns instantly, providing an added layer of security. Technologies such as continuous authentication are no longer a vision but a reality with AI.

Furthermore, endpoint protection has seen a transformation. Advanced AI-driven engines within ManageEngine offerings detect ransomware and malware with heightened precision. By analysing multi-dimensional behavior data, AI helps in assessing an organisation's security posture comprehensively.

In essence, while data's value grows exponentially, maintaining a proper security posture becomes paramount. ManageEngine recognises the indispensability of AI in ensuring topnotch security, guarding not just data but also an organisation's reputation.

COMMITTED TO EXCELLENCE AMIT KUMAR, MANAGING DIRECTOR AT MMA INFOSEC, TELLS ANITA JOSEPH HOW THE COMPANY IS FOCUSED ON COMPREHENSIVE CYBERSECURITY TRANSFORMATION IN THE REGION AND BEYOND.

ow would you describe MMA Infosec? MMA Infosec's core identity is rooted in an unwavering commitment to excellence. We are dedicated to fostering cyber resilience and preparedness, not just within our organisation, but also among our valued customers who join us on this journey towards excellence. To achieve this, we have strategically partnered with world-class leaders in the cybersecurity field, with the shared goal of becoming a cornerstone in our customers' pursuit of a cyber-proof future.

Where does MMA Infosec currently stand in terms of its product portfolio, and how do you determine what products are the best fit for your organisation?

MMA Infosec boasts a leadership team with over three decades of combined experience in both the cybersecurity and IT industries. This expertise positions us well to address the dynamic needs of today's customers while helping them plan for a more secure future. Our approach at MMA Infosec is evolving towards a comprehensive and proactive cybersecurity strategy, encompassing prevention, detection, response, and collaboration.

We are highly selective in the vendors we choose to include in our

portfolio. We are among the few in the industry that actively introduce new vendors to the region. We seek out customers who recognise the unique value in our offerings. Our commitment goes beyond a typical vendor relationship; we take full ownership, from operations and logistics to sales and marketing for our vendors. This level of investment is greatly appreciated by both our vendors and customers, as it underscores the exclusivity we bring to our portfolio.

How does MMA Infosec plan to fortify its position in the regional market?

Our vision at MMA Infosec revolves around strengthening our presence in the regional market by leading a comprehensive cybersecurity transformation while staying true to our mantra of being different and bold. Our strategy, which has proven successful over the past three years, involves establishing new branch offices across the Middle East. Simultaneously, we will continue to deliver added value to all our customers in each country we set foot in. As our customers attest to the uniqueness of our offerings and the quality of our work, our position in the market will naturally solidify over time.

Which industry verticals are crucial to MMA Infosec's business?

We specialise in serving industry verticals such as healthcare and critical infrastructure.

In a competitive market, how does MMA Infosec differentiate itself?

MMA Infosec stands out in the competitive landscape by prioritising proactive defense, detection, and response. Our overarching approach is proactive, not reactive, in everything we undertake.

What are the key advantages you offer your customers?

MMA Infosec provides several key advantages to our customers, including proactive resilience, comprehensive defense strategies that go beyond prevention, safeguarding societal interests, fostering collaborative networks with solution providers, and deep industry expertise. These advantages empower our clients to effectively navigate the everevolving landscape of cybersecurity challenges.

What revenue goals does MMA Infosec aim to achieve this year, and where do you envision the company in the next two years?

MMA Infosec is setting its sights on achieving double-digit revenue growth this year, driven by our innovative cybersecurity solutions. We believe that the sky's the limit for those who go above and beyond, and we are fully prepared to embrace the opportunities and challenges that lie ahead as we continue to grow.

WE WILL CONTINUE TO DELIVER ADDED VALUE TO ALL OUR CUSTOMERS IN EACH COUNTRY WE SET FOOT IN.



THE FUTURE IS HERE

G ITEX GLOBAL 2023, an annual convergence of the world's most innovative enterprises and brightest minds, promises to be a groundbreaking event that transcends boundaries and redefines the future. This year's theme, "The Year to Imagine AI in Everything," signifies a pivotal moment in the global race for AI supremacy. From October 8th to 12th, 2023, GITEX GLOBAL will ignite discussions and present expert perspectives that shed light on the profound impact of artificial intelligence on business, the economy, society, and culture.

At GITEX GLOBAL 2023, participants will embark on a journey into the heart of AI's transformative potential. Leaders, pioneers, and visionaries from various sectors will convene to share their insights, experiences, and strategies for harnessing AI's power. Attendees will gain access to the latest advancements in AI technology, witnessing firsthand the groundbreaking innovations that are shaping our future.

GITEX GLOBAL 2023 will also serve as a platform for networking and partnership-building. Enterprises, startups, researchers, and investors will have the opportunity to forge connections, exchange ideas, and initiate collaborations that will drive the AI revolution forward.

This year, GITEX GLOBAL isn't just an event; it's a journey into the future, a celebration of innovation, and a catalyst for change. Don't miss the chance to be part of this historic moment. Join us in imagining Al in everything and supercharging the epic global race for Al supremacy.

Here's a glimpse into what some of the exhibitors will display at the event:

A10 NETWORKS

10 Networks's participation will be centered around the theme of 'empowering regional enterprises with the most secure and available digital experience' by providing business-critical networks and applications that are secure, available, and efficient.

A10 will demonstrate its entire portfolio of on-premises and cloud-native security and infrastructure solutions designed to drive digital resilience and protect enterprise applications and infrastructure against cyber attacks. The company's focus will be on educating GITEX trade visitors about the latest and most innovative strategies and solutions to optimize, accelerate, and secure applications and networks for enterprises, service providers, and government organisations.

Amr Alashaal, Regional Vice President - Middle East at A10 Networks comments, "A10 helps secure critical service provider and enterprise networks against modern cyberattacks. In addition our solutions support efficient and effective cloud operating models with application security and availability, and simplify IT operations with connected intelligence, automation, machine learning, AIOps and DevOps/SecOps tools. We are looking forward to bringing these innovative technologies to GITEX, the world's largest tech show, and engaging in high-level discussions with both customers and partners."

During the event, Fatih Okumus, SE Leader, Middle East at A10 Networks will run a series of presentations delivered on the booth daily, with the intention of helping educate CIOs and IT managers about secure application delivery and access. In a world driven by digital applications, ensuring secure access and delivery has become paramount. These sessions highlight the pivotal role of SSL visibility systems, DDoS mitigation, and next-generation web



application firewall (WAF) technologies in safeguarding these crucial aspects of shifting security paradigms.

One of the technology highlights of A10's participation at GITEX this year is its recently launched A10 Next-Gen WAF, powered by Fastly, available as an integrated add-on to its A10 Thunder ADC solution. The combined technology enables a highly performant security solution at a strategic application ingress point that reduces false positives and automates security, empowering agility and effectiveness. The end solution ultimately helps secure web applications and deliver business outcomes.



AVAYA

vaya, a global leader in customer experience solutions, will illustrate how organisations can choose their own journey to delivering AI-powered customer experiences. The company will showcase a range of vertical-specific use cases that highlight the power of artificial intelligence (AI) in delivering outstanding experiences across the customer journey.

Throughout the week of the event, Avaya will demonstrate solutions that harness AI to reimagine the way customer and employee experiences are delivered. The solutions on display will also show how organisations can chart their own path to delivering these AI-enhanced experiences without disrupting existing operations.

SPOTLIGHT / GITEX

DATAIKU

t this year's GITEX Global, Dataiku will exhibit under the theme, "Maximising Business Value with AI: Scaling Across the Organisation". At a time when the region is displaying a notable uptick in the adoption rates of a range of AI technologies, we will use GITEX as a platform to showcase how our technology enables organisations to reap the maximum rewards from their AI investments by making AI accessible to users with varying skill sets and roles.

The company's GITEX 2023 focus will be on highlighting the features of the latest release of its flagship platform. Dataiku 12 offers integration with OpenAI's ChatGPT, allowing business users to incorporate the tool's learning models into their native data projects by extending datasets and performing tasks using a visual interface and natural-language prompts.

Version 12 also prioritises transparency and trust in project outputs, eliminating "black box" tendencies in Al through Transparent Automated Feature Generation. It introduces Causal Machine Learning (ML) to guard against the common analytical error of confusing correlation with causation, which can cause many different kinds of damage to the business and other stakeholders. Dataiku democratises these capabilities, ensuring that anyone building ML models can understand the source of results.



ID, the world's leading provider of trusted identity solutions, has announced that it will showcase its latest innovations in secure identity issuance and identity management at GITEX Global 2023 under the theme, "Secure, Sustainable, Future-proof Solutions".

Between 16 and 20 October, from Hall 5, Stand A15, at the Dubai World Trade Center, HID will demonstrate to GITEX delegates how the company has come to power the trusted identities of the world's people, places, and things.

HID will showcase the HID FARGO Connect — the industry's first cloud-native card issuance platform — paired with card printing innovations such as the HID FARGO HDP6600 retransfer card printer and the DTC1500 direct-to-card printer — to demonstrate how the solution simplifies card issuance while increasing security.

The company will also introduce its HID ELEMENT UV Ink Printer and Laser Engraver card personalisation solutions — specifically designed to meet the high-volume and high-security requirements of large organisations such as government entities and financial institutions.

Additionally, company experts will explain how HID PIAM (physical identity and access management) solutions reduce the costs and risks associated with onboarding, badging, visitor management, access management and compliance.

HID GLOBAL



NUTANIX

Will participate in GITEX Global 2023 for the 8th consecutive year, with the intention of helping regional organisations streamline operations and turn cloud complexity into multicloud simplicity. The company will share its vision and strategy of delivering the optimal hybrid cloud experience to radically simplify and solve the biggest modernisation needs of enterprise customers. The event will also serve as a platform to introduce regional customers to the 'World of Purple' - Nutanix's new brand identity that was unveiled at the company's flagship event .NEXT in Chicago in May this year.

The company is particularly excited about several announcements at GITEX. Starting off with the recent Global strategic partnership with Cisco. This partnership will combine Nutanix's best-in-class software with Cisco's SaaS managed compute portfolio to help our customers and prospects enter a hybrid multicloud future. The partnership with Cisco spans joint engineering and interoperability, expanded world-class support, goto-market cooperation for a more seamless customer experience, as well as building the foundation for broader solutions with Cisco's market leading networking, security and collaboration offerings.

Secondly, Nutanix announced Nutanix GPT-in-a-Box - a solution for customers looking to jump-start their artificial intelligence (AI) and machine learning (ML) innovation, while maintaining control over their data. The company believes there is a growing trend around the Al-powered edge. Organisations will begin to leverage public cloud resources to train AI models, but then deploy them at the edge, where the data is often collected. Most enterprises will not have the infrastructure or resources needed to train AI models in their own datacenter without huge investment, so they'll look to public cloud to supplement. This is where a hybrid multicloud strategy is even more important, as organisations will need a cloud platform that spans from public cloud, to their datacenters and the edge, to be able to move their applications and data where they're needed. Being able to manage and control both of these is hugely important.

Raif Abou Diab, Sales Manager, South Gulf & Pakistan at Nutanix said "The UAE has emerged as a shining example of a nation that has transformed its vision into a reality, positioning itself as a global leader in innovation, artificial intelligence (AI), and digital technology. We are proud to be able to support this vision through our ability to execute digital transformation efforts, as well as AI innovation with the recent announcement of Nutanix GPT."



RIVERBED TECHNOLOGY

hrough its participation at GITEX 2023, Riverbed will highlight how enterprises today and tomorrow can 'Deliver Exceptional Digital Experiences with Unified Observability and Acceleration'. Under this theme, its team will conduct live demos of Riverbed's flagship Unified Observability and Acceleration solutions for visitors to our stand.

Riverbed will also showcase its Alluvio Unified Observability portfolio which enables enterprises to capture every packet, flow, and end user transaction across multi-cloud and on-premises networks, applications, and user systems at full fidelity. By then applying intelligence through machine learning and artificial intelligence and automated investigative workflows, Riverbed's solutions help IT to quickly identify and resolve businessimpacting issues so organisations can maintain productivity and deliver on user experience expectations.





SolarWinds, a leading provider of simple, powerful, secure observability and IT management software, will present at booth H7-F50 alongside its valueadded distribution partners in the region — CyberKnight and Spire Solutions — showcasing its award-winning full-stack observability products, comprehensive database management portfolio, and service management solutions.

SolarWinds enables companies to manage increasingly

SOLARWINDS

complex hybrid and multi-cloud environments to accelerate digital transformation, drive automation, modernize applications, and undertake cloud migration initiatives. The company has further enhanced its solutions through the unified SolarWinds® Platform, providing customers with full-stack observability powered by AlOps, database, service management, security, and automation capabilities to identify and remediate issues and improve service delivery, reliability, and productivity — all while reducing costs.

Today, digital transformation and innovative technology are the main drivers of all industries and economies, which is why GITEX GLOBAL 2023 is extremely beneficial for our business. The trade fair is an ideal platform to tell the tech landscape what Al-powered innovations we offer to accelerate the digital economy," said Abdul Rehman Tariq, regional sales director, Middle East. "Our participation in the event reflects our commitment to the UAE market and is a great opportunity to demonstrate how SolarWinds and our value-added distribution partners in the region can help organisations accelerate their digital journey and drive enhancements in hybrid cloud and observability solutions."



enable, Inc., the Exposure Management company, will showcase its powerful Tenable One Exposure Management Platform, which harnesses the power of generative AI, putting more power than ever in the hands of security teams. Tenable One informs their exposure management programs to identify and remediate cyber risk wherever it exists. Tenable will also demonstrate its powerful operational technology security, cloud security and identity exposure capabilities.

Over the past year, record breaking data breaches have continued to dominate headlines and ransomware has cripplied the operations of numerous organisations. Organisations are battling to keep threat actors out of their infrastructure but are continuously in reactive mode. Tenable's approach turns

TENABLE

this around. Its exposure management platform combines broad exposure coverage spanning IT assets, cloud resources, containers, web applications and identity platforms, with threat intelligence and data science from Tenable Research. This helps focus efforts to prevent likely attacks and accurately communicate cyber risk to support optimal business performance.

"Too often, security teams are focused on identifying indicators of compromise, preoccupied with halting attacks before too much damage can occur. However, that's just too late. Once an attacker is inside the infrastructure, it's already game over," said Maher Jadallah, Senior Director Middle East & North Africa, Tenable. "At GITEX 2023, we want to show security teams how to gain the upper hand, helping them to change focus from constantly firefighting to proactively addressing their cyber risks. Our team will be on hand to help visitors understand how to refocus their efforts to prevent likely attacks. empowering organisations to accurately identify the risk their business faces and ultimately close the windows and doors attackers are climbing through."

Tenable will be co-exhibiting, alongside AmiViz from both H24-A40, Hall 24 (Cyber Valley), Ingram Micro from booth H2-A1, Hall 2 and Al Jammaz Technologies H2-C1, Hall 2. The Tenable Team will be offering demonstrations of its exposure management platform TenableOne, as well as Tenable Vulnerability Management, Tenable Security Centre, Tenable OT Security, Tenable Identity Exposure and Tenable Lumin.

t GITEX. Vectra will show how its new flagship platform can address the "spiral of more" — more attack surface, more sophistication in attack methods, more tools, more rules, more security analyst burnout.

At GITEX, Vectra AI will showcase the company's recently launched Vectra AI platform — a first-of-its-kind cybersecurity platform built for the modern hybrid environment. The Vectra AI Platform, with patented Attack Signal Intelligence, delivers the integrated signal enterprises need to optimise their investment in XDR.

Vectra's GITEX exhibit will feature demo pods highlighting each aspect of the company's new Al platform — Cloud Detection and Response, Identity Detection and Response, Network Detection and Response, Managed Detection and Response, Investigation and Threat Hunting, and Respond UX Powered by AWS.

VECTRA AI



IT TRENDS REPORT 2023: OBSERVABILITY ADVANCES AUTOMATION AND EMPOWERS INNOVATION

olarWinds, a leading provider of simple, powerful, secure observability and IT management software, released the findings of its 2023 IT Trends Report: Lessons From Observability Leaders. The report explores how enterprises can act proactively to maximise the advantages of their observability solutions, integrate best practices into implementations, and mitigate common adoption challenges. The report also found that companies implementing observability benefit from increased operational efficiency, faster innovation, and better business outcomes overall.

The new report is released in advance of IT Pro Day 2023, which falls on September

19 this year, and highlights a stark contrast between enterprises that have embraced observability and their peers who have not. Among the findings, the survey uncovered that observability leadersthose who follow best practices to leverage observability and report experiencing better business and IT outcomes as a result —are three times more likely to say their organisation is doing extremely well with growing revenue, more than twice as likely to say the same about operational efficiency, and 2.5 times more likely to say they're excelling with the speed of innovation. Observability leaders also gave higher ratings to their organisation's employee experience, including lower levels of reported employee burnout and fewer skill gaps on their teams.

These takeaways come at a critical time, as IT environments become increasingly complex, and companies experience more challenges in efficiently addressing IT issues as a result. According to the findings, the typical enterprise suffers from an average of nine brownouts or outages every month, lasting around twelve hours each, at an average annual cost of \$13.7MM. Observability has emerged as a solution to not only preemptively detect anomalies and potential issues before they escalate into full-blown outages but to proactively address those issues at the root cause and prevent future outages.

"Outages and security concerns are no longer just an IT problem, and observability is no longer just an IT solution," said Jeff Stewart, Field CTO and vice president, global solutions engineering at SolarWinds. "The better business, innovation, and technology outcomes experienced by observability leaders prove the benefits to every level, department, and employee. The findings of this year's report should serve as an urgent call to action for business leaders who believe they can't afford to invest in observability tools—when the truth is that we're rapidly entering a landscape in which companies simply can't afford to risk being without them."

The survey also highlighted trends among the observability leaders reporting fewer and less frequent challenges in their ecosystem, finding the majority are:

• Investing in top priorities:

Data shows organisations using observability solutions to support the priorities most critical to their growth and success: improve their customer experience (96%), enable faster innovation (71%), reduce time spent solving (71%), and detecting (60%) issues, and increase operational efficiency (55%).

More automated and integrated: Observability leaders embracing automation and investing in tools that provide enhanced efficiency are 214% more likely to say they are doing extremely well with operational efficiency, 750% more likely to say they are doing extremely well with autoremediation of complex alerts, and 300% better at automatically collecting background diagnostic data for IT support staff.



Ahead on IT: The data found that those ahead of the curve on observability are also leading by huge margins when it comes to monitoring, detecting, and resolving issues that could otherwise bring the business to a screeching halt. When it comes to IT, they are 233% better at auto-

OBSERVABILITY LEADERS ALSO GAVE HIGHER RATINGS TO THEIR ORGANISATION'S EMPLOYEE EXPERIENCE, INCLUDING LOWER LEVELS OF REPORTED EMPLOYEE BURNOUT AND FEWER SKILLS. GAPS ON THEIR TEAMS. escalation of tickets, 213% better at auto-remediation of simple alerts, and 36% better at settling alert levels based on historical behavior. SolarWinds offers its customers

full-stack observability solutions that provide organisations across all sizes and industries cost-effective, end-toend visibility and actionable intelligence to expedite remediation using powerful machine learning (ML) and artificial intelligence (AI) capabilities. These fully integrated, on-premises, and cloud-native SaaS solutions provide comprehensive visibility in hybrid and multi-cloud environments, including SolarWinds Observability and SolarWinds Hybrid Cloud Observability. **1**

CLOUD BOX TECHNOLOGIES ENHANCES ITS SECURITY PORTFOLIO WITH A STATE-OF-THE-ART SECURITY OPERATIONS CENTER

loud Box Technologies (CBT), a specialised IT services provider, has announced the launch of its cutting-edge Security Operations Center (SOC) in Dubai. The SOC, implemented by RA Technologies, a subsidiary of CBT, is primarily built to cater to local customer requirements. It is equipped with the latest technology tools to enable 24/7/365 threat monitoring, detection, and targeted response support, ensuring rapid identification and containment of security incidents. The SOC is also fully compliant with regulatory standards.

The role of RA Technologies is to offer expertise to safeguard customer networks against potential security breaches. The SOC utilises cuttingedge tools and technologies to detect any alterations in cyber threats and promptly respond with appropriate countermeasures.

The Security Operations Center (SOC) is capable to provide uninterrupted 24/7 surveillance for networks and IT infrastructure. Furthermore, it leverages internal threat intelligence knowledge base and also uses external data from partners and regulators to promptly detect, identify, investigate, and analyse cyber threats in real-time. Cybersecurity extends beyond risk management, and encompasses strategic aspects that influences product capability, organisational effectiveness, and customer relationships, based on unique customer requirements.

Ranjith Kaippada, Managing Director of Cloud Box Technologies said "As businesses are becoming increasingly connected, digital transformation of enterprises is inevitable. Leveraging our expertise in understanding customer's business, we are uniquely positioned to develop a comprehensive strategy, establish effective leadership, communicate a clear plan to management, and prepare the organisation to tackle the challenges of tomorrow."

"In recent times, there has been a substantial global investment in

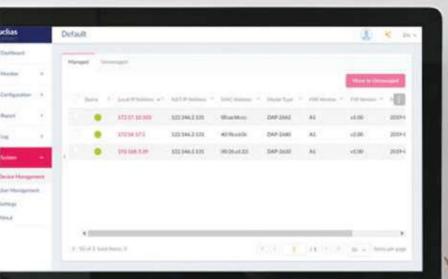
digital infrastructure. It is imperative to safeguard these investments from potential threats, and this is where a SOC plays a crucial role. We assess risks thereby enhance resilience which subsequently enhances the customer's security posture and facilitates efficient and heightened security capabilities." Kaippada added.

With the implementation of the new SOC, Cloud Box technologies is now capable of assisting their clients in formulating a comprehensive cyber strategy that encompasses the dimensions of risk, business, and culture. This will prove to be a valuable asset in their endeavours towards digitisation, as it will enable them to establish a secure environment.

Apart from staying ahead of cyber threats and damages, the SOC will also bring a curb on expenses associated with security breaches, help provide customers with frequent compliance reports, and aid in regulatory compliance with laws like HIPPA and GDPR. 1

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

< nuclias connect</pre>



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.



Wall-Plated Access Point

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



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

D-Link

1

DAP-2622

Nuclias Connect AC1200 Wave 2 Wall-Plate Access Point



Intelligent NDR Cyber Mesh Platform

— The New Approach to Cybersecurity Posture —

GLOBAL

.

0

e

STOP BY HALL #25-C60 16-20 OCT 2023

E: info@linkshadow.com T: +1 877 267 7313 W: linkshadow.com

0

Ø

0