

Security

ADVISOR

MIDDLE EAST



SPECIAL:
**CISO 50 & FSA
AWARDS 2022**

AI-DRIVEN SECURITY

IN AN EXCLUSIVE INTERVIEW, FADI SHARAF, REGIONAL SALES DIRECTOR AT LINKSHADOW, TELLS ANITA JOSEPH HOW THE COMPANY'S NEXT-GENERATION CYBERSECURITY ANALYTICS PLATFORM AUTOMATES THE DETECTION OF SOPHISTICATED ATTACKS WITH ANALYTICS-DRIVEN VISIBILITY.

Bringing IT together



**ManageEngine crafts comprehensive
IT management software for all your business needs.**

Identity and access management | Enterprise service management | Unified endpoint management and security | IT operations management | Security information and event management | Advanced IT analytics | Low-code app development

Trusted by



**Top 5
airlines**



**6 of the biggest
oil and gas companies**



**Top 10
GCC banks**

ManageEngine

www.manageengine.com

Phone: +971 4 574 8400 | Email: sales@manageengine.com

Visit us at

GITEX
GLOBAL

10-14 October 2022

#H7-C1, Hall 7

Dubai World Trade Centre

CONTENTS



- | | |
|--|--|
| <p>6 Top headlines from the security industry in the region and beyond.</p> <p>8 Toufic Derbass, Managing Director, Micro Focus, on the company's participation at GITEX and the Hybrid Cloud Management X platform.</p> | <p>28 Glimpses into the CISO 50 Forum & Awards and the Future Security Awards held recently.</p> <p>38 Gopan Sivasankaran, General Manager, META at Secureworks, on the company's growth in the past year, its cutting-edge XDR platform and participation at GITEX.</p> |
|--|--|



Digital Security
Progress. Protected.

Proven Multilayered Security



Modern Endpoint
Protection



Advanced
Threat Defense



Full Disk
Encryption



Cloud App
Protection



Mail Security



Detection &
Response



ESET MIDDLE EAST

For more information visit:
eset.com/me or Contact sales@esetme.com
ESET MIDDLE EAST at GITEX 2022 - Hall 1, Stand H1-E1

EDITOR'S NOTE



Talk to us:

E-mail:

anita.joseph@cpimediagroup.com

Anita Joseph
Editor

THE FUTURE IS HERE

Cyber-attacks are rising at an exponential rate, and we are experiencing varying trends that are highly strategic and meticulously planned. It is becoming imperative for enterprises to implement newer and robust approaches to building a resilient infrastructure. The crucial question here is - Are we better protected today than yesterday? CISOs and security teams must up their game and work in-tandem to ensure consistent control over multiple factors such as tackling the biggest cybersecurity risks, protecting the business operations, identifying where lies the vulnerabilities and most importantly what returns are they receiving from their IT investments.

Our cover story in this issue has Fadi Sharaf, Regional Sales Director, LinkShadow, tell us how the company steps in with its next-generation cybersecurity analytics that offers enhanced defences against advanced cyberattacks. He is of the opinion that their unique solution architecture has capabilities that equips organisations to address zero-day malware and ransomware and simultaneously provide rapid insights into the effectiveness of the security infrastructure and risk posture.

Our interview of the month spotlights

another important aspect of security: MDR. Gopan Sivasankaran, General Manager META at Secureworks discusses how a good MDR provider must have strong XDR fundamentals in place and how a buyer can evaluate an MDR provider to make sure he's getting what he really needs.

Not to be missed are snapshots from the CISO 50 Forum & Awards and the Future Security Awards held last month.

A hugely successful gathering of security decisionmakers saw debates around planning for an effective cybersecurity roadmap and how CISOs can change the mindset of organisations to focus more

on the business value that security can bring. The Future Security Awards saw the security trendsetters being celebrated for their futuristic and innovation-centric initiatives and decisions.

We've also brought for you glimpses of what GITEX, the region's biggest technology event, has in store this year. All the who's who of the security world will converge at the Dubai World Trade Centre to offer best-in-class technology and security solutions and lead the way into a bright, exciting and unpredictable future.

Make no mistake, this issue of your favourite magazine is power-packed. Enjoy, Happy Reading!

NEXT-GEN SECURITY

EVENTS



FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by **CPI**

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

EDITORIAL
Editor
Anita Joseph
anita.joseph@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehanjan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

OnlineEditor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

© Copyright 2022 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.

SWIMLANE EXPANDS INTO MIDDLE EAST, TURKEY AND AFRICA

Swimlane, the low-code security automation company, has announced

its expansion to the Middle East, Turkey and Africa (META) with the appointment of Ashraf Sheet as Vice President of the region. Sheet will build on the increasing demand for Swimlane security automation throughout META while accelerating the company's go-to-market and channel growth plans in the region.

According to a report, globally, there is already a shortage of some 2.72 million cybersecurity professionals, and a critical need for the workforce to grow 65% to effectively defend organisations' assets. When you consider that the Middle East cybersecurity market on its own is projected to more than double from US \$20.3 billion in 2022 to \$44.7 billion by 2027, driven by significant government economic diversification drives, it's fair to say that the recruitment of cybersecurity professionals from within the region or from international markets, will continue to significantly challenge organisations.

"Ashraf brings immense credibility and go-to-market experience throughout META, and I'm excited to have him lead Swimlane's expansion in the region," said Jim Pickering, Senior Vice President of Worldwide Sales for Swimlane. "Our unique low-code approach to security automation is a game-changer for security teams in META, offering a solution that meets the region's most-demanding and constantly evolving security operations requirements."



F5 NAMED BEST-IN-CLASS FOR BOT MANAGEMENT IN AITE-NOVARICA MATRIX OF LEADING BOT DETECTION AND MANAGEMENT PROVIDERS

F5 has announced that Aite-Novarica

Group, a financial services research and advisory firm, has ranked the company as a Best-in-Class provider of bot management solutions in their recently released Aite Matrix: Leading Bot Detection and Management Providers report.

As a Best in Class vendor, F5's approach integrates bot and fraud detection capabilities to secure organisations from a breadth of automated attacks while reducing user friction and allowing for the continued operation of good bots. "We're thrilled that Aite-Novarica Group has recognised F5's Distributed Cloud Bot Defense as Best in Class," said Haiyan Song, Executive Vice President and General Manager, Security & Distributed

Cloud at F5. "Bots aren't going away anytime soon—in fact, they will only continue to get more prevalent and sophisticated. That's why, in order to ensure a secure and frictionless digital experience for users, bot management solutions must automatically and intelligently adapt as attackers retool to bypass countermeasures. We're aiming to do just that with our solution strategy to converge bot management, app security, and fraud detection capabilities, and it's great to see the results and the recognition of our unique approach."



TEXUB TO SHOWCASE INNOVATIVE GLOBAL B2B MARKETPLACE AT GITEX GLOBAL 2022

TEXUB has announced its participation

in GITEX Global 2022, the region's premier technology exhibition. The company will showcase its innovative global B2B marketplace – a safe, stable and seamless trade ecosystem for global IT trade, and demonstrate how it digitally connects verified B2B sellers and buyers from all around the world. TEXUB will also introduce its 'DigiNOMICS' program, which offers training for sales personnel to specialize in digital sales and help accelerate digital transformation.

"Since TEXUB was launched earlier this year, we have received tremendous response from both buyers and sellers from across the globe. GITEX Global 2022, being one of the biggest ICT exhibitions globally, is an ideal forum for us to create a better face-to-face awareness of TEXUB's unique value proposition of pioneering the future of IT trade. Our participation

in this mega exhibition helps us showcase our platform as a true IT and mobility marketplace, highlight our new training program – DigiNOMICS, and demonstrate to buyers and sellers how easy it is to onboard their products and transact. We look forward to amplifying our message to a wider audience visiting GITEX from across the world," said Suchit Kumar, CEO of TEXUB.

"Beyond GITEX Global 2022, we will continue to provide the market with information on our progress as TEXUB aims to become a global operator in the IT trade sector," he added.

TEXUB will be at Stand 32 in Hall 4. Senior executives and experts from the company will be available to meet with visitors.





STARLINK
LEADS
WITH AN INSPIRING CULTURE

MANAGING THE HYBRID MULTI CLOUD

TOUFIC DERBASS, MANAGING DIRECTOR, MICRO FOCUS,
ON THE COMPANY'S PARTICIPATION AT GITEX AND THE HYBRID
CLOUD MANAGEMENT X PLATFORM.

GITEX 2022, the much-awaited technology event, is here. How is Micro Focus making its presence felt at the show? What new solutions/products can we look forward to?

We're looking forward to meeting our customers and partners at GITEX this year. It's great to be present at such a gathering of technology companies from all over the region. We'll have 2 meeting rooms in Hall 3 with Micro Focus VIP Lounge to host and meet our clients-to discuss, debate and challenge new ideologies. We acknowledge global changes in our customers' need to move fast with digital transformation, but keep running their businesses in parallel. We call it run and transform at the same time.

Tell us about Micro Focus' Hybrid Cloud Management X platform.

In recent years, companies around the world increased the adoption of cloud to support the Work From Home movement, lower their capital expenditures, and gain the speed and agility that cloud enables.

While the benefits of cloud are undeniable, we also have to address the disruption and complexity to the IT ecosystem-the hybrid, multi cloud ecosystem. Challenges include deficient governance controls and spiralling cloud costs – average overspending is estimated at over 30%.

Micro Focus Hybrid Cloud Management X or HCMX, was built to resolve these challenges. It is an industry leading solution,





highly regarded by analysts and customers alike.

With HCMX you can expect to:

- 1) Significantly lower your cloud spend
- 2) Speed-up multi-cloud infrastructure provisioning, and
- 3) Ensure compliance with policy-based controls

What is the USP of this new platform?
How will it help enterprises in their digital transformation journey?

HCMX enables IT to design deployment-ready, full-stack environments across on-premise technologies and public clouds. It unifies and automates provisioning, day 2 life cycle operations and de-provisioning, making sure you're governing the entire life cycle of those hybrid cloud services. Those services are delivered to end users with a unified self-service portal for on-demand consumption.

BASED ON AI, HCMX WILL PROVIDE YOU WITH SMART INSIGHTS AROUND RESERVED INSTANCE MANAGEMENT TO HELP YOU OPTIMISE USAGE & SPEND ON PUBLIC CLOUDS.

These offer an alternative approach to catalogue browsing, and guide end users to quickly find IT-approved offerings. On the other hand, HCMX provides strong governance and cost control, including flexible approval management, advanced cost reporting and granular budget management. Add to that, built-in Machine Learning capabilities to enable intelligent insights around reserved instance management, to help our customers optimise their usage and spending on public cloud.

HCMX is an enterprise-grade solution that supports you at scale, provides multitenancy, and can be deployed as SaaS, on-premise, or also on Hyperscalers. Unify your multi-cloud and on-premise operations, lower cloud spending, speed up provisioning, and ensure compliance – with automation and AI built-in. To get more information on HCMX, please follow this link:

<https://www.microfocus.com/en-us/products/hybrid-cloud-management-x/overview> 

Fast. Reliable. Secured
SWITCHING SOLUTION



Save Energy **without**
SACRIFICING PERFORMANCE

DGS-F1210-26PS-E

Layer 2 Gigabit Managed Long Range PoE+ Switch



Highlights

- Superior connectivity
- Maximum distance of 250m
- Plug-and-play installation
- High Availability & Comprehensive Security
- Flow control for protection against data loss
- Suitable for devices that are far from power outlets
- New Value-Engineered Series to Meet today's Infrastructure Needs

D-Link®

Connect to more...



THE CHALLENGE OF SHARED RESPONSIBILITY IN THE CLOUD – WHOSE KEYS ARE THEY, ANYWAY?

SEBASTIEN PAVIE VP DATA PROTECTION PRODUCTS, SOUTHERN EMEA AT THALES

Key management – the processing, management and storage of keys for who can decrypt and access protected information – is an often-overlooked, and yet critical element of encryption. Many organisations left that part up to their vendors or stored them inconsistently across their IT infrastructure in both hardware and software. This lack of centralized control can jeopardize the integrity of encryption. In fact, the management of the keys is more important than the encryption itself,

because if something happens to the keys, entire sets of data can be stolen or lost, and there's nothing you can do about it.

The fact that major cloud heavyweights are diving into this technology is a sign that key management is being taken more seriously. And rightly so. The ability to demonstrate control of data is critical to meeting compliance mandates. But how do you really own your data if you do not have total control and ownership of the keys?

With every passing day, an increasing number of organisations are migrating their sensitive data and business applications

to the cloud for operational flexibilities, cost efficiencies and quick scalability. To avoid vendor lock-in on a single cloud service provider (CSP), like Microsoft Azure, AWS, Oracle Cloud, and IBM Cloud, many organisations are opting to work with multiple CSPs in a multi-cloud environment.

As an increasing amount of critical data gets stored in the cloud, the prospect of cyber-attacks and data breaches rises exponentially. While most CSPs offer native data protection features, the "Shared Responsibility Model" dictates that the ultimate onus of safeguarding business and



Discover

Data Discovery
Data Classification
Risk Assessment



Protect

Data Encryption
Key Management
Hardware Security Modules



Control

Access Management
User Access Controls
Multi-Factor Authentication

Data Security for a Zero Trust World



customers' sensitive data rests with organisations. While there is a shared responsibility to secure data in the cloud, there is no shared liability and the impact of potential security incidents jeopardising sensitive data remains the responsibility of the company and it is the company's responsibility to ensure compliance with the relevant privacy regulations such as the GDPR, the Schrems II ruling, PCI-DSS, HIPAA or CCPA.

While organisations are increasingly investing in perimeter security mechanisms, they fail to adequately invest in encryption technologies that act as the critical line of defence in the event of a cyber-attack. This is evident through the ever-increasing incidents of sophisticated cyber-attacks that

result in data breaches costing organisations billions in losses.

To minimise the impact of potential security incidents and to optimise sensitive data protection, security and privacy regulations like GDPR, PCI-DSS, HIPAA or CCPA mandate the adoption of encryption.

However, merely encrypting sensitive data in the cloud is not sufficient. The Cloud Security Alliance recommends as an industry best practice for storing information in the cloud to put the customer in control of both the key management and the encryption process. Effectively managing the key lifecycle and being crypto-agile is paramount for establishing trust in the confidentiality, integrity, and availability of your data.

To that extent, the EU Cybersecurity Agency (ENISA) points out that client-side encryption is the only way to provide the customer with true control over their data, while mitigating the risk of an unauthorised access by third parties. NIST SP 800-144 adds that organisations should be "in control of the central keying material and configure the key management components for cloud-based applications."

Barriers to multi-cloud data protection

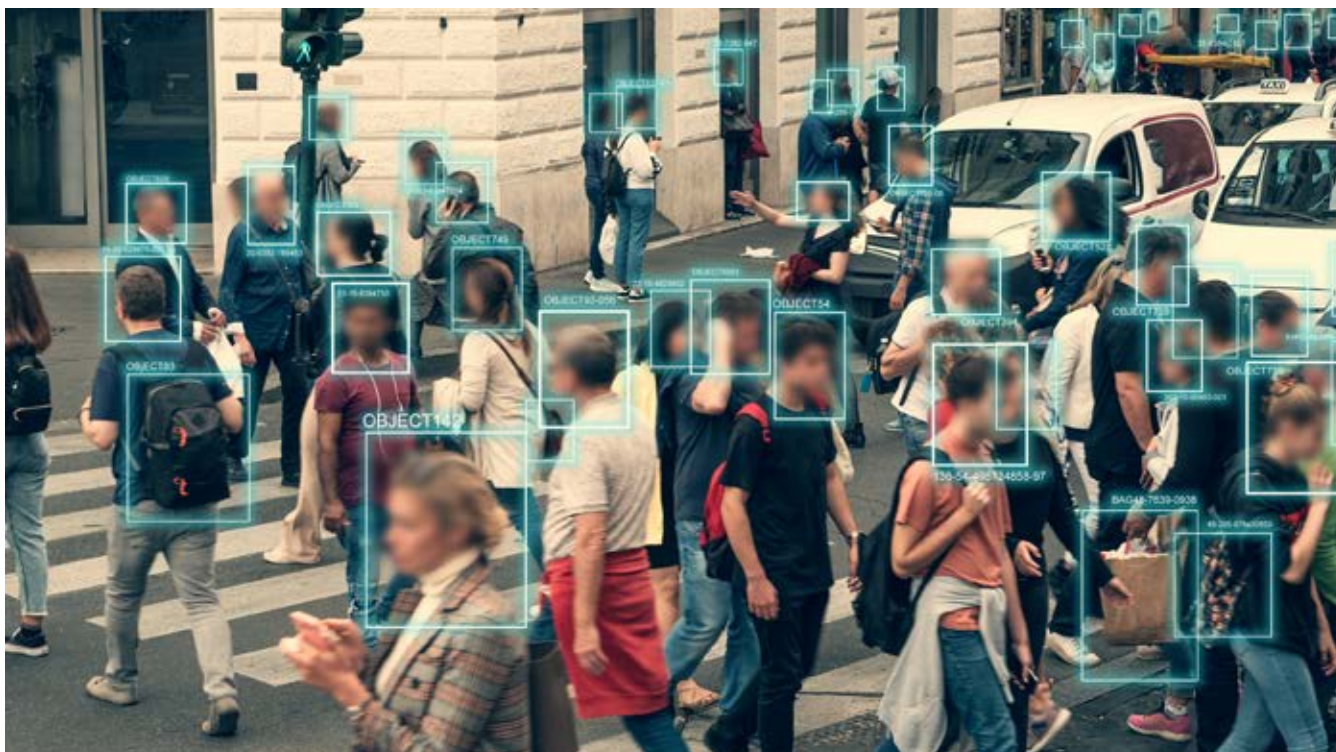
When it comes to cloud security and efficient key management, there are a number of major pain points organisations face today that prevent them from taking full advantage of the potentials offered by cloud platforms.

1. Lack of visibility into security and encryption practices.

With CSPs providing limited visibility and access on encryption practices and schemes, organisations' risk management teams are reluctant to allow the storage of sensitive and mission critical data in the cloud due to high impact in case of a data breach.

2. Meeting compliance requirements.

Security and privacy regulations mandate



the use of state-of-the-art practices for securing the confidentiality and integrity of personal and sensitive data, requiring agility and strong control over key management. Lack of such controls entail big regulatory penalties.

3. Managing encryption keys across multiple cloud environments.

Organisations are embracing multi-cloud strategies to avoid vendor lock-in. The use of cloud-native encryption and key management solutions is a barrier to multi-cloud adoption.

4. Custodianship of encryption

keys. When organisations elect to use cloud-native encryption services, the corresponding keys are being managed by the providers. Not having direct control

on the keys presents potential risks and vulnerabilities in the case of a security or cryptographic incident.

5. Managing, monitoring, and deploying multiple cloud native security tools. Since cloud-native key management services offer limited ability to automate the lifecycle of encryption keys, especially across multiple subscriptions, organisations are forced to implement labour-intensive, error-prone manual key management processes to meet their security requirements.

The right approach to cloud data protection

Lack of proper security and key management practices in a multi-cloud environment will only increase

the organisation's attack surface, with cybercriminals eager to take advantage of it as they get smarter and more sophisticated. Luckily, there are many industry best practices, such as Bring Your Own Key (BYOK), Bring Your Own Encryption (BYOE) and centralised and automated key lifecycle management that can optimise data protection in the cloud.

With cloud providers being responsible for the security "of" the cloud, and organisations having responsibility for the security of their data "in" the cloud, every CISO should ask the five pertinent questions below:

1. How do I maintain strong security controls of my cloud assets?
2. Post-migration, what key management controls do I need?
3. How do I manage my personal and sensitive data risks?
4. How do I manage my audits?
5. How do I meet regulatory compliance?

Cloud security is important for your business prosperity. Thales's multi-cloud security solutions offer a cohesive answer to each of these questions. Please visit our website for more information. 

WHILE ORGANISATIONS ARE INCREASINGLY INVESTING IN PERIMETER SECURITY MECHANISMS, THEY FAIL TO ADEQUATELY INVEST IN ENCRYPTION TECHNOLOGIES THAT ACT AS THE CRITICAL LINE OF DEFENCE IN THE EVENT OF A CYBER-ATTACK.

CLOUDFLARE ANNOUNCES FIRST ZERO TRUST SIM FOR MOBILE DEVICES

NEW MOBILE OPERATOR PARTNER PROGRAM WILL ALSO ENABLE ANY CARRIER TO BUNDLE ZERO TRUST SECURITY INTO EXISTING CORPORATE PLANS



Cloudflare, Inc, the security, performance, and reliability company helping to build a better Internet, has announced the development of the

Cloudflare Zero Trust SIM, the first solution that secures every packet of data leaving mobile devices. With the Zero Trust SIM that Cloudflare is developing, organisations will be able to quickly and securely connect employee devices to Cloudflare's global network, directly integrate devices with Cloudflare's Zero Trust platform, and protect their network and employees no matter where they are working from. Additionally, Cloudflare will be launching Zero Trust for Mobile Operators, a new wireless carrier partner program that will allow any carrier to seamlessly offer their own subscribers comprehensive mobile security tools by tapping into Cloudflare's Zero Trust platform.

"When I speak to CISOs I hear, again and again, that effectively securing mobile devices at scale is one of their biggest headaches, it's the flaw in everyone's Zero Trust deployment," said Matthew Prince, co-founder and CEO of Cloudflare. "Effectively securing mobile devices is hard, and we have been working on this problem since we launched our WARP mobile app in 2019, now we plan on going even further. With Cloudflare Zero Trust SIM we will offer the only complete solution to secure all of a device's traffic, helping our customers plug this hole in their Zero Trust security posture."

CLOUDFLARE ZERO TRUST SIM WILL INTEGRATE SEAMLESSLY WITH CLOUDFLARE'S ENTIRE ZERO TRUST STACK, ALLOWING SECURITY POLICIES TO BE ENFORCED FOR ALL TRAFFIC LEAVING THE DEVICE.

As organisations have become more distributed with remote working and employees bring their own device (BYOD) to work, ensuring every device employees use is secure is harder than ever. To help with this problem, most organisations use a secure agent, or application, running on an employee's device to help secure it. However, while applications and endpoint agents are an important part of the security stack, they can't secure all traffic across every device, and can be challenging to deploy at scale. To help fill this gap Cloudflare is developing the Zero Trust SIM, the industry's first zero trust solution to secure mobile employee devices at the SIM level, protecting every packet of data.

Cloudflare Zero Trust SIM will integrate seamlessly with Cloudflare's entire Zero Trust stack, allowing security policies to be enforced for all traffic leaving the device. Further, with the Zero Trust SIM taking an eSIM (embedded SIM) first approach, SIMs can be automatically deployed to both iOS and Android devices and locked to a specific device, mitigating the risk of SIM-swapping attacks faced by existing solutions and saving security teams time. With the Cloudflare Zero Trust SIM businesses will be able to:

- **Secure every packet leaving employee devices:** Software agents are imperfect and may not be able to handle every type of traffic. Because every data packet leaving a device goes over the SIM,

Cloudflare Zero Trust SIM will be able to help secure all of an organisation's data.

- **Deploy at enterprise scale in minutes:** Building on modern eSIM technology means that the Zero Trust SIM will be able to be automatically deployed and enabled using existing MDM (Mobile Device Management) solutions across all devices within an organisation, allowing them to seamlessly roll out Cloudflare's Zero Trust SIM without the pain of shipping physical SIM cards.
- **Integrate Seamlessly with Cloudflare WARP:** The Zero Trust SIM will be able to be used standalone or deployed with WARP, Cloudflare's mobile agent, to enable device posture controls and HTTPS inspection for organisations with more demanding needs.
- **Secure the Internet of Things:** As more and more objects connect to the Internet, from vehicles to payment terminals and shipping containers to vending machines, these devices need to be secured as well. Cloudflare is currently developing new tools, based on the Zero Trust SIM, to provide industry leading connectivity and Zero Trust security for the Internet of Things.

Cloudflare also announced the Zero Trust for Mobile Operators program as part of Cloudflare's efforts to help enterprises secure mobile devices. The wireless carrier partner program aims to jointly solve the biggest security and performance challenges of mobile connectivity. By combining Cloudflare's award-winning security tools with the largest mobile networks in the world, businesses can be confident that their devices and data are secure without worrying about performance being impacted. 📶

CISCO APPOINTS SAYED HASHISH AS VP OF CUSTOMER EXPERIENCE FOR MEA

IN HIS NEW ROLE, **HASHISH** WILL HELP SHAPE CISCO'S STRATEGIC CX DIRECTION IN MEA, WITH A STRONG FOCUS ON LEVERAGING TECHNOLOGY TO SUPPORT DIGITISATION, INNOVATION AND SOCIAL INCLUSION.

Cisco has announced the appointment of Sayed Hashish as Vice President for Customer Experience CX, Middle East & Africa, succeeding Adele Trombetta who was promoted to Vice President for CX, EMEA in late 2021.

Hashish, a 24-year technology veteran of Microsoft, brings more than three decades of diverse experience in executive leadership and digital transformation to the wider region.

Prior to joining Cisco, Hashish was General Manager, Microsoft UAE, where he spearheaded planning and growth initiatives that enabled and empowered digital transformation in the UAE. Before that, he was Regional General Manager for Microsoft Gulf where he successfully launched the company's Middle East Cloud regions.

In his new role, Hashish will help shape Cisco's strategic CX direction in the Middle East & Africa, with a strong focus on leveraging technology to support digitisation, innovation and social inclusion. He will help build customer loyalty and ensure customers take full advantage of Cisco's software, services, and subscription offerings.



CX is one of Cisco's largest business units, and a key growth engine for the company's transformation to a recurring revenue business model.

Adele Trombetta, Vice President, Customer Experience, EMEA, said: "I am delighted to have Sayed lead CX in the Middle East and Africa. With decades of experience in the technology sector, he will

help accelerate our transformation strategy and drive further growth in the region."

Commenting on his appointment, Hashish said: "I am thrilled to join Cisco. I have always admired the trust Cisco enjoys from its customers and partners which uniquely positions us to drive digital transformation with our customers and enable the Middle East and Africa region to take full advantage of opportunities technology creates. I feel privileged to be part of the Cisco's transformation journey and support the team in building great capabilities that unleash market potential and accelerate growth."

Hashish holds a Bachelor of Science in Physics from the American University in Cairo. 🇪🇬

CX IS ONE OF CISCO'S LARGEST BUSINESS UNITS, AND A KEY GROWTH ENGINE FOR THE COMPANY'S TRANSFORMATION TO A RECURRING REVENUE BUSINESS MODEL.



Keep cybercrime out of your inbox.

Protect your business from phishing
and ransomware with Barracuda
Total Email Protection.

Visit Barracuda at GITEX 2022.

Dubai World Trade Centre
10th - 14th October

Stand No: H1 - C20

AI-DRIVEN SECURITY

IN AN EXCLUSIVE INTERVIEW, **FADI SHARAF**, REGIONAL SALES DIRECTOR AT LINKSHADOW, TELLS ANITA JOSEPH HOW THE COMPANY'S NEXT-GENERATION CYBERSECURITY ANALYTICS PLATFORM AUTOMATES THE DETECTION OF SOPHISTICATED ATTACKS WITH ANALYTICS-DRIVEN VISIBILITY.

LINKSHADOW 
Combat the Dark

In a world where the threat landscape is rapidly evolving, the need for new approaches to cyber security are becoming extremely important. How does LinkShadow approach this scenario?

Cyber-attacks are rising at an exponential rate, and we are experiencing varying trends that are highly strategic and meticulously planned. It is becoming imperative for enterprises to implement newer and robust approaches to building a resilient infrastructure. The crucial question here is - Are we better protected today than yesterday? CISOs and security teams must up their game and work in-tandem to ensure consistent control over multiple factors such as

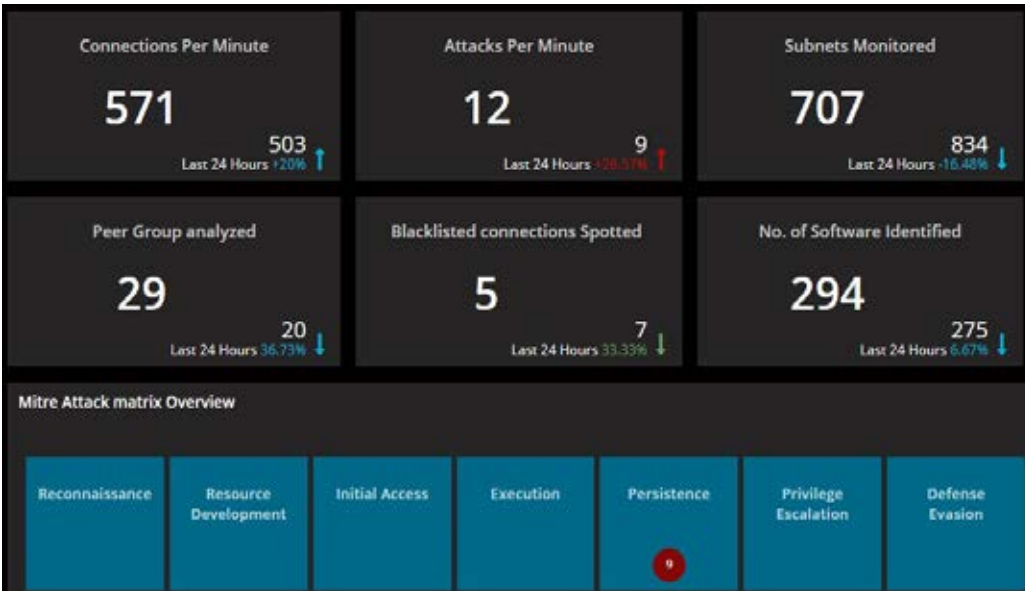
tackling the biggest cybersecurity risks, protecting the business operations, identifying where lies the vulnerabilities and most importantly what returns are they receiving from their IT investments.

Whilst racing to keep cybercrime in check, identifying and investing in the right security tools has never been an easy task for the cybersecurity community. Deploying too many technologies does not mean it is the best strategy to prevent breaches. Traditional technologies may be inadequate to deal with more sophisticated cyber-attacks. Therefore, enhancing infrastructure with a modern methodology that helps organisations stay secure, vigilant, and resilient at the same time is much in demand.



What LinkShadow Next-Generation Cybersecurity Analytics offers is enhanced defences against advanced cyberattacks. The solution architecture is designed to manage threats in real-time with user and entity behavioral analytics (UEBA) and extensive machine learning (ML) capabilities to detect both insider and external threats. With these capabilities, organisations would be equipped to address zero-day malware, ransomware and simultaneously have a rapid insight into the effectiveness of the security infrastructure and risk posture.

→ **ENHANCING INFRASTRUCTURE WITH A MODERN METHODOLOGY THAT HELPS ORGANISATIONS STAY SECURE, VIGILANT AND RESILIENT AT THE SAME TIME IS MUCH IN DEMAND.**



Tell us about LinkShadow’s threat detection capabilities.

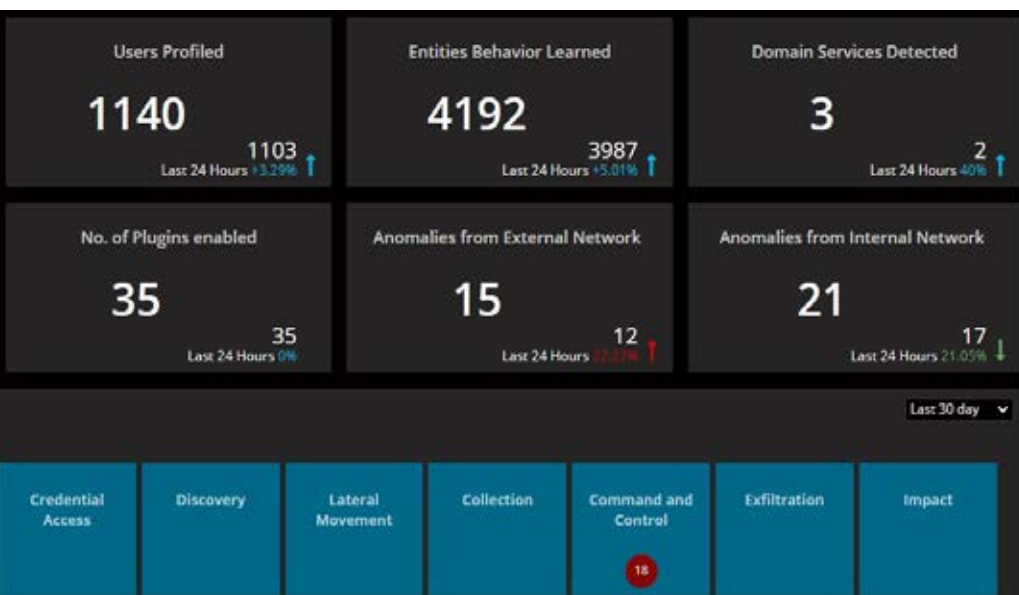
Staying 100% protected from a cyber-attack can be a far-fetched vision. However, organisations can protect their infrastructure with security tools that can help detect and mitigate threats before they cause serious damage. It is a known fact that attacks involving compromised users and entities are extremely complicated to detect because adversaries can evade perimeter

defences by using legitimate credentials to access data.

Implementing advanced threat detection techniques that can address unknown threats, reduce alert fatigue, and integrate security tools is key and though it sounds like a big task, it is possible with the right mix of threat detection and response processes.

LinkShadow next-generation cybersecurity analytics platform automates the detection of these





attacks with analytics-driven visibility. The advanced techniques include supervised and unsupervised machine learning which are applied to data from the network and security infrastructure (e.g., packets, flows, logs, alerts). This information is used to create threat scores for all users and entities and distinct security events are observed & correlated over time. These advanced attacks that might appear to be legitimate user activity which could be an attacker posing as a legitimate insider are identified by measuring the changes and/or the anomalies associated with each entity. It takes smart correlation of the orphan alerts, over a period to detect such anomalies. Moreover, the platform also provides one-click access to the historic data to gain perspective whilst

investigating the attacks.

LinkShadow delivers a differentiated analytics solution by combining machine learning with layered forensics, which automates attack detection and incident

investigation without rules, configuration, and signatures.

LinkShadow has a unique Solution Architecture. Tell us more about it.

LinkShadow's solutions architecture is a full-fledged behavioral analytics and extended threat hunting platform covering network, assets and users that is designed to hunt, detect, and prevent known or unknown threats using advanced machine learning algorithms. It provides rapid insights to cut through the noise of daily alerts and helps in drastically curbing response times. It comprises of three main modules – Insights, Behavioral Analytics and Threat Hunting that essentially assists security teams with:

- Network Detection and Response
- User and Entity Behaviour Analytics
- Network Threat Hunting
- CXO Dashboards and Reporting
- Threat Intel

**LINKSHADOW
DELIVERS A
DIFFERENTIATED
ANALYTICS
SOLUTION BY
COMBINING MACHINE
LEARNING WITH
LAYERED FORENSICS.**



These enhanced threat intelligence and advanced analytics capabilities combined enables an enterprise-wide security program that is proactive and predictive.

One of the core modules which is the Threat Hunting Module is driven by an AI-powered engine that helps detect the most sophisticated attacks and visually map them to the Cyber Kill Chain and MITRE ATT&CK frameworks to combat ransomware, security breaches and advanced persistent attacks (APTs) whilst giving end-to-end visibility and control over the ML algorithms from Data Collection to Detection to Visualisation.

Why is LinkShadow unique? – Because of its capabilities to seamlessly integrated with multiple solutions – be it SIEM solutions or other cloud security providers that can be deployed from an in-house API plugin store which has most of the known technologies, at no additional cost. Thereby, empowering customers to build a highly resilient cybersecurity infrastructure with this holistic solutions approach. It can be positioned on-cloud or on-prem with a one-time buy or subscription-based

LINKSHADOW'S NEXT-GENERATION CYBERSECURITY ANALYTICS PLATFORM INTERACTS SEAMLESSLY WITH CLOUD APPLICATIONS, ALLOWING USER INTERACTIONS TO BE PROCESSED AND MONITORED IN REAL TIME.

licensing model. This makes LinkShadow an easy choice for organisations as it is convenient to adapt into their existing IT Infrastructure.

Cloud Security is huge today and it requires a specialised, expert approach. How is LinkShadow helping clients with Cloud security?

Cloud adoption has become integral to modernising the IT environment for large enterprises as well as SMBs and with this implementation a huge amount of data is being stored in the cloud. All that data is a top target for cyber criminals who can intercept an organisation's security system within minutes or even seconds, to steal this sensitive data and by the time

the security teams discover the breach, it could take hours, sometimes even days or weeks – by then irreversible damage is already done.

Multiple platforms like the public, private and hybrid cloud are deployed which makes it difficult to monitor data, detect anomalies and control unauthorised access. Protecting the cloud environment from cyber-attacks is highly dependent on the type of security controls and analytics tools an organisation has in place that helps analyse the data to obtain actionable insights and prevent future attacks.

LinkShadow's next-generation cybersecurity analytics platform interacts seamlessly with cloud applications, allowing user interactions to be processed and monitored in real time, whether they originate inside the network or from remote locations. LinkShadow's AI-powered engine simplifies the complexity of Machine Learning and AI-based tools by empowering security teams to have full control over the entire threat hunt process and helps them stay ahead of threat adversaries. Moreover, it curates threat intelligence and applies advanced Machine Learning models to provide rapid insights, refines meaningless information enabling drastic reduction in response times and facilitates periodic access reviews to detect anomalies proactively and avoid breaches.

How has LinkShadow established its presence in the Middle East and what expansion plans are in the pipeline?

LinkShadow emerged from a compelling dream that a team of highly skilled and



LINKSHADOW'S SOLUTIONS ARCHITECTURE IS A FULL-FLEDGED BEHAVIORAL ANALYTICS AND EXTENDED THREAT HUNTING PLATFORM.



passionate experts envisioned – which was to enhance organisations defences against advanced cyber-attacks, helping them stay one step ahead of the increasingly evolving threat adversaries as well as ensure that they can maximise their security investments. Right from the beginning our focus was to innovate and cater to our customers unique cybersecurity requirements. Our growth trajectory is due to the innovation that we bring to the technology, especially with our R & D teams based out of this region that helps us develop cutting-edge cybersecurity solutions.

The company kick-started expansion plans in this region with the launch of the Dubai office, our innovation hub that will accommodate up to 100 plus R & D experts. So, in terms of space and resources

LinkShadow would be one of the largest cybersecurity vendors based out of the UAE. However, our META hub would be in Riyadh, KSA, which we will be launching shortly.

No doubt, LinkShadow is growing exponentially, and is all set to establish its presence in this region with the aim of establishing closer partnerships with the channel community as well as ensure quicker turnaround and faster implementation to customers.

GITEX being one of the largest technology shows in the META region, how do you plan to leverage from this in exclusive platform? What new offerings does LinkShadow have for the customers and the channel community?

Organisations are adopting digital transformation, which has raised the

capabilities of attackers and increased their appetite to exploit organisations, systems, infrastructure, and applications. Therefore, it is crucial to continuously monitor and classify every asset and their related threats and vulnerabilities, to understand and anticipate adversaries' entry points to the organisation and defend against malicious activities.

At LinkShadow, we are constantly on the pursuit of enhancing our solutions architecture so organisations can keep their IT infrastructure secure and enable them to focus on business operations, uninterrupted.

This GITEX, we have launched a new feature called 'Attack Surface powered by Metaverse'. With this feature, LinkShadow aims to empower organisations monitor, discover, and recommend security best practices for various infrastructure components to provide defenders with a complete understanding of their attack surface across all assets at any given time.

Moreover, security and compliance teams will have a complete toolset to understand and mitigate risks across their associated attack surface. It enables organisations to see the blind spots visible to adversaries and move the advantage back to security teams to eliminate any expected attack on their infrastructure whilst actively interacting with resources, threats, and prospect attackers through a reliably rich virtual space. 🔑



ESET TO SHOWCASE PRODUCTS THAT PROTECT ENTERPRISES IN THEIR DIGITAL JOURNEY

THE ESET PROTECT PLATFORM HAS BEEN ENHANCED WITH ESET'S CUSTOMERS IN MIND, WITH THE MAIN OBJECTIVE BEING IN ASSISTING IT ADMINS TO BETTER MANAGE SECURITY RISKS.



ESET, Europe's leading global-scale digital security provider, has announced its participation at GITEX Global 2022, where the company will highlight its new refreshed line of business products that ensures enterprises in the Middle East can embark on a secure and a smooth digital journey and prevent cybercriminals doing any damage to their networks.

Demes Strouthos, General Manager at ESET said: "ESET has been a pioneer in the digital security and we have part of several organisations in the region to keep their assets, employees and data safe for decades. With our refreshed line of business products organisation can be sure

of running their networks smoothly and securely, so that their digital journey is not hampered in any which ways."

ESET Inspect Cloud

ESET Inspect Cloud is a sophisticated cloud-based tool, which enables the ESET PROTECT platform to evolve into an Extended Detection and Response (XDR) solution for enterprise-grade security and risk management capabilities, including advanced threat hunting, incident response, full network visibility, cloud-based threat defence, and more. ESET Inspect Cloud identifies post-execution malicious code, while ESET PROTECT gives the user full visibility of the response.

ESET PROTECT

The ESET PROTECT platform has been enhanced with ESET's customers in mind, with the main objective being in assisting IT admins to better manage the security risks in their environments. Firstly, an auto-update mechanism ensures that all ESET Endpoint agents and implemented solutions are always up to date, lightening the burden on IT admins' shoulders. Secondly, an in-depth integration of ESET Inspect Cloud and the ESET PROTECT platform allows for a much smoother experience, with sleeker dashboards and more streamlined deployments. Furthermore, ESET PROTECT will now offer a dashboard for ESET LiveGuard Advanced, an advanced threat defence solution with cloud sandboxing included within one of its layers, that analyses suspicious files submitted by endpoints for new or previously unseen threats.

"GITEX has always been a wonderful platform to connect with partners, customers, industry experts, ad at the same time from all across the world. We look forward to yet another successful GITEX and take this opportunity to interact with peers and showcase our cutting-edge technology during the weeklong show," Demes added.

Visitors at the GITEX Global 2022 can reach out to us at Stand No. H1-E1 in Hall 1 and can engage with the ESET leadership team to understand how our solutions can ensure they can embark on a smooth digital journey and prevent cybercriminals from playing havoc with their networks. 📍

Simple. Powerful. Secure IT.

- » Over 300,000 customers in 190 countries from SMB to Fortune 500®
- » 499 of the Fortune 500 are customers
- » #1 in Network Management*
- » 50+ IT management products

solarwinds.com

* IDC Worldwide Network Management Software Tracker 2H 2020.

Come visit us at GITEX!

October 10 – 14 | Dubai | H7-F30



OBSERVABILITY



NETWORK
MANAGEMENT



SYSTEMS
MANAGEMENT



DATABASE
MANAGEMENT



IT SERVICE
MANAGEMENT



IT SECURITY



APPLICATION
MANAGEMENT



tahawultech.com
**FUTURE
SECURITY**
Awards 2022

HONORING THE SECURITY FRONTRUNNERS

The security industry has always been in a never-ending race against its adversaries, but in the last two years in particular, the rate of change has accelerated. While companies continue to invest in technology and layer more systems into their IT networks to support digital transformation, resulting in potential new vulnerabilities, adversaries have been leveraging powerful, integrated tools and capabilities with artificial intelligence and machine learning, to hit and 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 individuals, businesses, and vendors that have risen above challenges and delivered ground-breaking 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. The awards welcome companies from across the Middle East. It acclaims the best security minds and projects in the region whose technologies, products or solutions are deemed to have a great potential in meeting the needs of the rapidly transforming digital era.



Best Cloud Solutions Vendor of the Year

Barracuda Networks

DDoS Protection Vendor of the Year - A10 Networks



Best Identity and Access Management Vendor of the Year

ManageEngine



Best Cybersecurity Training Provider of the Year

SANS Institute



Best Cybersecurity Solutions Partner of the Year

CNS Middle East



Best Endpoint Security Vendor of the Year

Sophos



Best Security Systems Integrator of the Year

Cloud Box Technologies



Best Security Distributor of the Year

Redington Gulf



Best Data Privacy Consulting Partner of the Year

Protiviti



Best Smart Home Security Vendor of the Year

EZVIZ



Innovative Smart Home Security Solutions Provider of the Year

Ring



Best AI Security Vendor of the Year

Hikvision



Best Edge-to-Cloud Security Vendor of the Year

Aruba, a Hewlett Packard Enterprise company



Best Threat Intelligence Vendor of the Year

Kaspersky



Best Managed Detection and Response Vendor of the Year

Secureworks



Best Data Security Firewall Vendor of the Year

Gajshield



Best Cloud Security Vendor of the Year

Acronis



Innovative XDR Solution of the Year

Trellix



Best Security Vendor of the Year

SolarWinds



Best Enterprise Email Security Vendor of the Year

Mimecast



Best Network Security Vendor of the Year

LinkShadow



Best Managed Security Services Provider of the Year

Help AG



Best Cybersecurity System Vendor of the Year

Raqmiyat



Best Cybersecurity VAD of the Year

Bulwark Technologies



Best Security Value Added Distributor (VAD) of the Year

StarLink



Disruptive Security VAD of the Year

Exclusive Networks



tahawultech.com

CISO 50

FORUM & AWARDS 2022

*Celebrating ExCellence
in Security leadership*



PADAM SUNDAR KAFLE
Aster Hospitals UAE



**RAMAKRISHNAN
NATARAJAN**
Emirates Hospitals Group



AFFEEF VEETIL
Invest Bank P.S.C



**JASON DHAKAN
SANAD**



MAY DASHTI
Gulf Bank, Kuwait



FAISAL AL QUBAISI
Emirates Red Crescent



**MOHAMMAD AHMAD
ALOMARI**
Solutions by STC



ABDULRAHMAN KHAIWI
Emirates National Schools
(ENS)



MOHAMMED MUNIB
National Bonds Corporation



**MANIVANNAN
NAGARAJAN**
Mashreq Bank



ABDULRAHMAN SHALABI
ENOC LLC



SHAFIULLAH ISMAIL
Mubadala Capital



LALIT AGGARWAL
ETG World



GIGI MATHEW THOMAS
Ittihad International
Investment



ALOK TUTEJA
Aghia PJSC



VISHAL BHAWNANI
DU Telecom



ASHISH KHANNA
Dubai Health Authority



RAMADAN MOHAMAD ALI
Ajman Transport Authority



ZAHEER SHAIKH
Al Maryah Community
Bank LLC

AISHA AWADH ALHEMEIRI of Department of Community Development
UMESH MOOLCHANDANI of Bin Dasmal Group
PRASAND GOPAKUMAR of RAK Public Service Department
FAHAD QURESHI of Talabat
ABDUR RAHMAN HUSSAIN of Islamic Development Bank
MANOJ KUMAR of Anantara the Palm Dubai Resort
MAGDY EL HAWARY of ASGC Group
NITHIN GEO THOMAS of Amity University Dubai
ANOOP PAUDVAL of Gulf News Al Nisr Publishing
SALWA SHAHEEN of The Shared Electronic Banking Services Company (KNET)
SHABEER MOHAMMED of GEMS Education
AMER AL HAFI of Dubai Financial Market
MOHAMMED DARWISH AZAD of Emirates NBD
KAJJAL MUSTAFI of Sharaf Exchange

 **tahawultech.com**

CISO 50
FORUM & AWARDS 2022



ABDULLAH BARWANI
Omantel



JAYESH NANDANAN
Mediclinic Middle East



SUFIYAN AL SHARIF
Dubai Media Incorporated



JACOB JACOB DEWA



MOHAMMED AMINUDDIN
Investcorp, Bahrain



SUNG PONG
Bank Muscat, Oman



KHALID OTHMAN BINAHMAD
Solutions by STC



ARUN MENON
Network International



HADI ANWAR
CPX



MOHAMMED SULTAN ALOLAMA
Emirates Health Services



HAMDA SAEED ALMAAZMI
MOHAP



AHMED AL ZAROUNI
Investment Corporation of Dubai



AHMAD AL-SUGHAYER
Cybersecurity Department
Kuwait National Guard



MOHAMMAD HENNAWI
NAFFCO



ABDULLA BADER AL SAYARI
Department of Health



NORMAN ANGELO QUIMIO
Horizon Geosciences

THE RIGHT KIND OF SKILL

 **CHRIS DALE**, PRINCIPAL INSTRUCTOR AT SANS INSTITUTE, ON CYBER DECEPTION, CYBERSECURITY, THE THREAT LANDSCAPE AND MORE.

What's your take on the threat-security landscape today?

For a long time, cybersecurity has been a bane to organisations. It seems like it is inevitable that we will never really protect ourselves fully. We see companies with large digital footprints and vast security budgets get hacked, but also smaller organisations with seemingly nothing to hide or steal.

Attackers in the threat landscape today find value in targeting both. A large corporation is an interesting target because they often hold valuable data, can pay larger ransoms, and have more systems to provide value to attackers. Smaller organisations are also valuable to attackers as they can be targeted in larger quantities. While perhaps the value of the target is lower, by targeting small organisations in larger quantities, it can offset the value accordingly.

Value in compromise come through data or processing capabilities. Smaller companies often think they can go under the radar, but with fewer security capabilities it often enables attackers to hack them more easily. On the contrary, larger organisations have more budgets to spend, but due to larger footprint may give attackers more avenues of finding vulnerabilities to exploit. Companies, large or small, still struggle with the most critical security controls: knowing themselves, which assets and which software they manage.

To make things worse, unfortunately, people are most often targeted and used as an entry point into the inside of an

organisation. Attackers are continuing to target our employees but are being deterred by more commonly used security controls such as Multi-Factor Authentication (MFA). This does not however prevent the attackers from abusing our people, as they are starting to utilise more clever techniques in bypassing said control. Attacks combined with social engineering attacks and other vectors which render MFA to be less effective are rapidly on the rise.

It has been a long time since attackers were known for making mistakes that could easily be pierced by attentive employees. The modern-day attacker is educated, trained and well capable of not being restricted by today's security controls. Vendors are known to quickly respond to the latest hacks with how their solutions could have prevented them but unfortunately they are proven wrong by security professionals time after time.

You recently authored a new SANS Course; can you tell us about it?

Cyber Deception is quickly becoming a great security strategy to help flip the coin on attackers. It is often said that attackers must be successful once, but defenders must succeed every time. Cyber Deception aims to arm defenders with a flip of the coin. Using deceptive controls, we can attempt to force the attacker's hand to reveal themselves. This makes the attackers have to be successful every time, otherwise they risk being detected by high fidelity alerts. The SEC550: Cyber Deception – Attack Detection, Disruption and Active Defence course seeks





to arm cyber defenders with the skills necessary to create such detective controls and furthermore allow a strategic approach on how cyber deception can help produce actionable threat intelligence on attackers trapped in a web of lies and deception. What are attackers looking for? What is their mission, and what are their capabilities? Cyber deception allows us to seek and produce such answers.

The class supports students in thoroughly understanding what cyber deception capabilities can give us. It shows us how it is a control that can easily be implemented to complement existing security controls, but also for advanced operations where deception can disarm attackers, giving defenders time and opportunity to respond accordingly.

Today, it is imperative for organisations to not only find the right cyber talent with specific skill sets, but also invest in continuing skill development. How does SANS help with this?

There are many ways through which SANS supports organisations to find the right talent and equally how we help cyber talent take the necessary steps to become an even better version of their current selves. Our cyber academies are a good example, but

THE MODERN-DAY ATTACKER IS EDUCATED, TRAINED AND WELL CAPABLE OF NOT BEING RESTRICTED BY TODAY'S SECURITY CONTROLS.

our cyber ranges also offer interactive and educational ways to hone ones' skills.

But mostly, SANS hosts a wide variety of free and accessible material for everyone to seek knowledge from. These resources are made by industry experts and are provided for free, as part of giving back to the community. Furthermore, SANS produces some of the highest standards of course materials and instructors in the industry today. We have a comprehensive roadmap for training new talent into security roles, ranging from introductory classes for security novices to the advanced classes only applicable to the most elite participants.

In your opinion, what's the biggest challenge to effective security implementation, in organisations?

I see many organisations suffer from patch and alert fatigue. We have too many things to patch, but not enough information to know where to start. Additionally, sometimes patches break functionality, giving us extra concerns when rolling them out, often causing us to patch too late.

Alert fatigue is a different aspect where we see security operations being flooded with too many alerts, too little actionable information and with skill gaps preventing staff from thoroughly investigating and concluding alerts. The security workforce in many cases is not empowered or given enough time to properly understand alerts and improve security controls and alerts to be more applicable for the future.

We must also take lessons from the offensive way of thinking. Think like attackers. Offensive must inform defence. If organisations focus on core aspects such as knowing themselves and knowing the attackers (and their skills and capabilities), the defence should not have to fear a "hundred battles," to quote Sun Tzu. The information and training is available out there, but can we change ourselves to make changes fast enough? 🧑‍💻

**Next-Generation
CyberSecurity Analytics**

VISUALISE & MONITOR YOUR SECURITY POSTURE WITH

Attack Surface

— Powered by —
Metaverse

Detect Cyber and
Insider Threats

GITEX
GLOBAL

**STOP BY HALL #2
10-14 OCT 2022**

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

ON THE SECURITY FRONTLINES

IN A SPECIAL INTERVIEW WITH SECURITY ADVISOR, **GOPAN SIVASANKARAN**, GENERAL MANAGER, META AT SECUREWORKS, TELLS ANITA JOSEPH ABOUT THE COMPANY'S GROWTH IN THE PAST YEAR, ITS CUTTING-EDGE XDR PLATFORM AND PARTICIPATION AT GITEX.

What can we look forward to from Secureworks at GITEX?

This year, we'll be present along with our partner Redington Value, and the spotlight will be on our XDR capabilities. There's a lot of ambiguity around XDR-the common perception is that it's a combination of SIEM & EDR, which is not the case, and GITEX will give us the perfect opportunity to create awareness about what it actually is. We'll also focus on other key areas such as consulting, penetration testing and Incident Response (IR), among others.

Tell us about your partnership with Redington Gulf. What's the synergy like?

There are two facets to this relationship. We benefit from the scale that Redington provides, with its extensive regional presence and massive partner ecosystem, which helps strengthen our narrative. Redington Gulf, on its part, leverages the Secureworks Taegis platform to power its recently-launched 'DigiGlass' brand, which, in turn, ensures that we deliver on our vision of ensuring that Taegis XDR is at the heart of every SOC.

MDR SHOULD BE BUILT ON SOUND XDR TECHNOLOGY.

MSSP partners are important for Secureworks and Redington Gulf is our valued MSSP partner, using our platform to deliver their services. Therefore, this synergy is significant for both of us.

What has the last one year been like for Secureworks?

It was a phenomenal year where we saw growth and expansion at every level. I've completed a year in my new leadership role with Secureworks in the region, and in that period, we witnessed remarkable progress across all fronts. In the channel space, we signed up with Redington Gulf and elevated the relationship to the next level. We also grew in terms of headcount, hiring key resources in South Africa and witnessing business growth in emerging Africa. We hired our first employee in Bahrain, who also looks after Kuwait, and appointed a Saudi national for Saudi Arabia. In fact, in

the last 12 months, we hired around 13 people-a growth of around 50-60% in terms of headcount.

Our XDR revenues also rose significantly and we signed on some key MSSP partners. We received public references-customer advocacies-where CISOs discussed how they were able to enhance their SOC operations with the Secureworks platform.

Looking back, it's been a productive and extremely rewarding year.

Let's talk security-MDR in particular. With so many MDR players in the market, how do you think a buyer can evaluate a provider and make sure he's getting what he really needs?

MDR should be built on sound XDR technology. It's important to realise that you cannot deliver good MDR service without having a solid XDR platform. Contrary to what many believe, a SIEM solution with an EDR or MDR rolled into it does not make it MDR-that's just a stunted version of it and nothing more.

This makes it essential to fully comprehend XDR as a concept before getting into MDR-it's like having a big data lake where you collect raw telemetry





instead of just getting alerts. An EDR forwarding an alert to a SIEM is unlike raw telemetry being forwarded to a big data analytics platform, and that's a massive difference.

That said, the 'R' in MDR represents response. So, a buyer would need to really understand how good a provider's Incident Response team is-what their qualifications are, whether they have the skill sets required to handle a breach, how good they are from a detection and investigation perspective, how much threat intelligence visibility they have, what kind of threat research they're doing, how good they're with threat hunting-all of this is extremely vital.

Today, everyone claims to be an XDR provider-they're all being forced into this space because of the huge demand there-so it's important for a buyer to carefully sift through these aspects.

Why choose Secureworks as an MDR provider?

There are two reasons for this. The first is that we have an open XDR platform, which

LOOKING BACK, IT'S BEEN A PRODUCTIVE AND EXTREMELY REWARDING YEAR.

WE HAVE AN OPEN XDR PLATFORM, WHICH MEANS WE DO NOT RIP AND REPLACE WHATEVER INVESTMENTS A CUSTOMER HAS MADE.

means we do not rip and replace whatever investments a customer has made. This also implies that we can work with other network security controls, whether it's Palo Alto, or Crowd Strike or FireEye, and will not force customers to use the Secureworks controls. Customers find this convenient, because other security providers almost always force them to use their agents and security controls.

The second reason is that we've been doing SOC for 22 years, so we understand this better than anyone else. Also, our service mindset is unique. Most of the MDR providers today are technology companies that got into the service business in the last 2-3 years. But for us, service is our DNA and we've been doing this for a really long time, so we have a clear advantage.

There are the two key differentiators among many others, that make Secureworks stand out from the rest.

Secureworks has a lot of plans for the region going forward. Can you tell us about some of them?

One of the things we're doing globally and I'm replicating in my region, is that

we're tapping the mid-market. We used to be an enterprise-class solution and not affordable for the mid-market space till a few years ago. Not anymore. We're now saying that security is not only for enterprises, but also for everyone else. In fact, it's becoming increasingly clear that it's time for the mid-market to invest in security, because this segment is progressively becoming targets of business email compromise and other kinds of fraud. So, Secureworks is stepping in to become affordable for the mid-market.

Another aspect is our improved focus on the channel. Since we're growing beyond the niche space we used to operate in and diversifying into the large, mid-market segment, we need our partners now more than ever, to grow further. I started with two employees in the region 9 years ago, now we're thirty-one. We're not just hiring sales and pre-sales personnel but also expanding our channel and our delivery organisation with presence in Incident Response, Penetration Testing, Program Management and Customer Success Management- we continue to hire these team members in the region, locally. 📍

logitech®



THE NEW LOGIC OF WORK

Hybrid Work,
Equitable Meetings and
The New Logic of Work



**SECURITY.
STABILITY.
SIMPLICITY.**

Introducing Logi Bolt
next-generation wireless
connectivity

RADWARE LAUNCHES CLOUD SECURITY CENTER

RESPONDS TO REGIONAL DEMAND FOR LOW LATENCY PERFORMANCE AND COMPLIES WITH OFFSHORE DATA ROUTING REQUIREMENTS.



Radware, a leading provider of cyber security and application delivery solutions, has announced the launch of a new cloud security center in the United Arab Emirates. Located in Dubai, the facility will reduce latency for in-region traffic and offer customers faster mitigation response times against denial-of-service attacks, web application attacks, malicious bot traffic, and attacks on APIs. It will also mitigate compliance processes involved in offshore routing.

The Dubai addition complements

THE NEW SITE IN DUBAI FILLS A GROWING DEMAND FOR A LOCAL SECURITY PRESENCE THAT CAN DELIVER RAPID RESPONSE TIMES WITH ACCURACY FOR ORGANISATIONS IN THE PUBLIC AND PRIVATE SECTORS.

Radware's existing cloud security network. Today, the network includes over 10Tbps of mitigation capacity across more than 50 security centers located around the globe.

"As part of our strategic cloud services initiative, we continue to accelerate cloud

innovation to provide our customers with the highest level of cyber security services," said Haim Zelikovsky, vice president of cloud security services for Radware. "This includes increasing the fighting capacity of our cloud infrastructure to help our customers manage the increasing complexity and sheer volume of cyberattacks with as little disruption as possible."

According to Radware's First Half 2022 Global Threat Analysis Report, the first six months of 2022 saw a dramatic increase in cyberattacks across the globe. The number of DDoS attacks climbed 203% and malicious web application transactions grew by 38% compared to the same period last year.

"The new site in Dubai fills a growing demand for a local security presence that can deliver rapid response times with accuracy for organisations in the public and private sector," said Nikhil Karan Taneja, Radware's vice president and managing director for India, the Middle East, and South Asia. "The launch of the center underscores our ongoing commitment to delivering state-of-the-art cyber protection and scaling our capacity in a way that will benefit the whole region." 🧑



COMMVAULT® 

Be **data** ready.

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

commvault.com



A COMPREHENSIVE SECURITY FRAMEWORK

JOE EL KHOURY, DIRECTOR – CYBERSECURITY, RAQMIYAT LLC, TELLS ANITA JOSEPH IN AN EXCLUSIVE INTERVIEW HOW RAQMIYAT HELPS CUSTOMERS ACHIEVE THEIR IT SECURITY VISION, STARTING FROM THE USER TO THE NETWORK, TO THE APPLICATION, AND FINALLY TO THE DATA.

How would you describe the cybersecurity landscape in the region today?

Ransomware continues to be a major threat in the UAE. UAE businesses have experienced a greater number of ransomware attack in the last 12 months which resulted in major damages to the organisation. According to a survey, 84% of UAE companies paid the ransom in these attacks, which is more than 20% higher than the global average. Of the companies that paid, 90% experienced a second ransomware attack and 59% found their data corrupted. Public Infrastructure Systems and Government IT systems have become a target of choice for hackers. As in the news, malicious actors, backdoors, commodity ransoms, etc are all knocking government agencies and financial institutions across. The UAE is rolling out several digitisation initiatives and they are also aware of the new threats associated with digitisation-the nation is well prepared for that. Threat actors will continue to leverage new techniques and organisations should be aware of what to expect. RansomOps will likely start moving toward the exfiltration and encryption of cloud data. Use of the cloud has grown, especially since the pandemic, and as a

result, RansomOps are searching for vulnerabilities to target on platforms like AWS and Azure.

What are some of the threats that are prevalent in the region now, post the pandemic?

Post-pandemic, many organisations were forced to rapidly adapt to meet new challenges and the cyber threat actors were taking advantage of this shift, cloud adoption is rising with a remote workforce and companies are trying to cope with the scalability and accessibility offered by those solutions. While companies are moving to the cloud, security is lagging since cloud infrastructure is different from the traditional data center. Phishing is getting more sophisticated, and the attacks are using machine learning to distribute more convincing fake messages, the ransomware strategies are evolving and allowing hackers to deploy advanced technologies to encrypt data.

Connected devices are opening doors for IoT attacks and create a greater attack surface-more devices mean greater risk. The cryptocurrency movement is also affecting cybersecurity in other ways, where the crypto-jacking trend plays a role in hijacking computers for cryptocurrency mining.



moving forward, as cybercriminals become more sophisticated, the cybersecurity professionals suffer a severe shortage that intensifies the cyberthreat.

Tell us about Raqmiyat's cybersecurity portfolio. What is the focus of your offerings?

We offer comprehensive cyber security solutions and services that help organisations secure their assets from malicious threats and improve overall security and cyber-resiliency. We deliver real value to customers and partners with our vendor-agnostic and technology-centric security framework. By using our framework, customers are able to comprehensively achieve their IT security vision, starting from the user to the network, to the application, and finally to the data. We help decision-makers to quickly and easily

visualise multiple security domains to help understand, prioritise, and mitigate risk. We offer our solutions and services covering areas such as Threat Protection, Incident Response, PIM/PAM/Identity Management, Multi-factor Authentication, database activity monitoring, network access control, Email security, secure mobility/EFT, Infrastructure Security, Data protection, Identity & Access Management, Risk & Compliance, Security Intelligence Center, and Managed Security Services.

How does Raqmiyat help organisations achieve cyber resiliency and mitigate risk?

Achieving cyber resilience has become a challenging task because in recent years, there has been a clear rise in threat volume and cybercriminals moved to sophisticated techniques to evade detection

and target high value assets. The lack of real-time visibility for the enterprise security status associated with IoT devices has become a focus for threat related to credential harvesting and ransomware. This trend needs an effective cybersecurity risk mitigation strategy that limits the impact of successful attacks. Raqmiyat offer organisations to achieve their security target and create security policies and processes to reduce the overall risk of a cybersecurity threat. We separate the risk mitigation into three main sections: Prevention, Orchestration and Recovery and we adapt the cyber risk mitigation for the organisation to always maintain an upper hand.

What is your advice to organisations looking to strengthen their cybersecurity infrastructure?

The first would be to bring in real-time visibility of business exposure due to cyber risks. The other factors would be to draw a correlation between the ROI of cyber investments and losses owing to cybersecurity, detect and eliminate overlapping security technologies and bring in near real-time visibility and transparency on business exposure. 📌

THE LACK OF REAL-TIME VISIBILITY FOR THE ENTERPRISE SECURITY STATUS ASSOCIATED WITH IOT DEVICES HAS BECOME A FOCUS FOR THREAT RELATED TO CREDENTIAL HARVESTING AND RANSOMWARE.

Fortinet Security Fabric

Broad

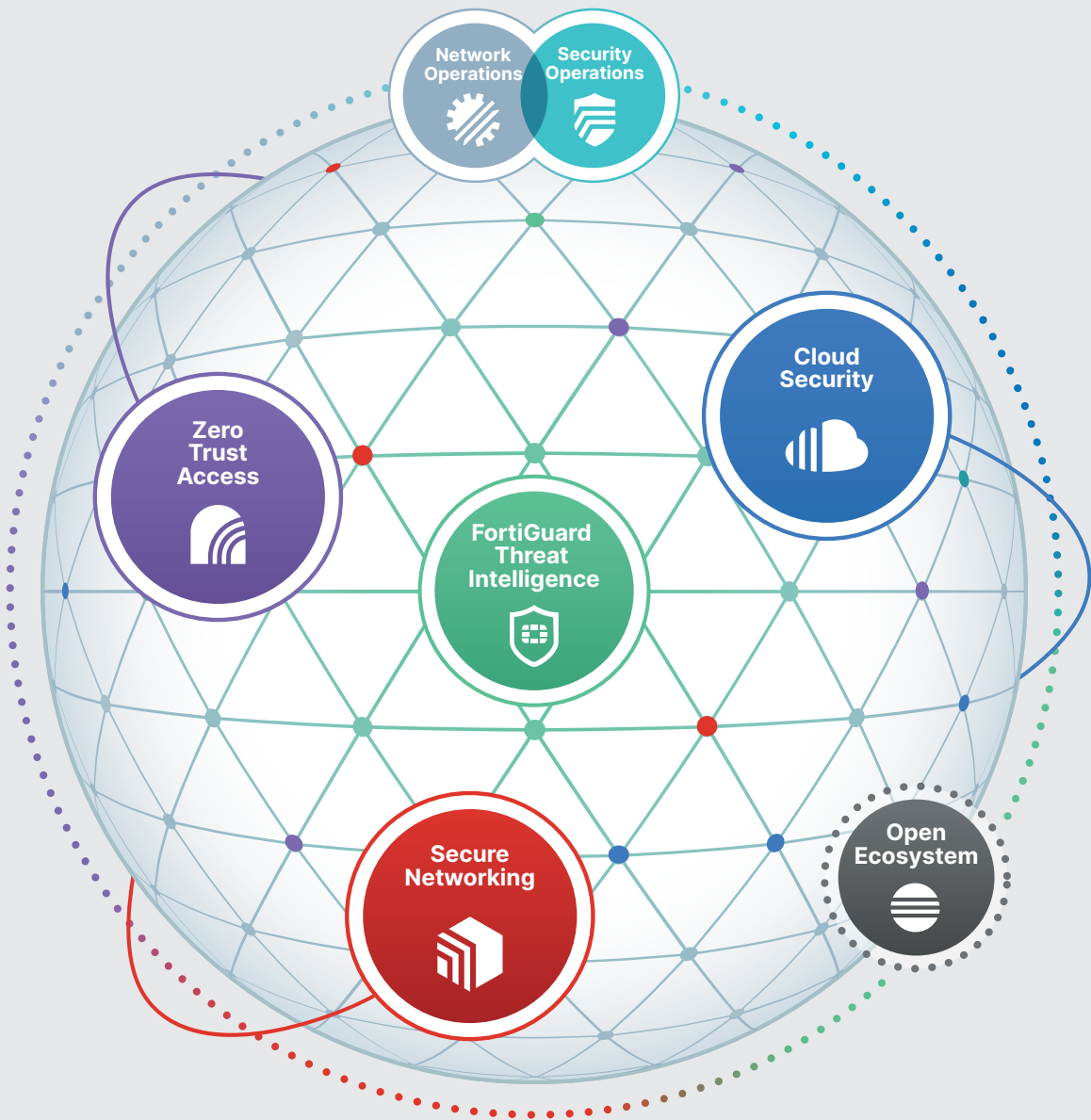
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with AI-driven security for fast and efficient operations





ANITA JOSEPH CAUGHT UP WITH **BRANT SHEN**, GENERAL MANAGER - UAE, OMAN & YEMEN AT DAHUA TECHNOLOGY, ON HOW THE COMPANY IS LEADING THE WAY WITH ITS FUTURISTIC PORTFOLIO OF PRODUCTS AND SOLUTIONS.

Tell us about Dahua Technology and its portfolio of products and solutions.

Dahua Technology is a world-leading video-centric smart IoT solution and service provider. Committed to its mission of “enabling a safer society and smarter living,” Dahua Technology offers end-to-end security solutions, systems, and services to create value for city operations, corporate management, and consumers.

The company has more than 22,000

employees, of which over 50% are engaged in R&D. Committed to technological innovation, the company invests approximately 10% of its sales revenue to R&D every year. It has established Advanced Technology Institute, Big Data Institute, Central Research Institute, Cybersecurity Institute, and Smart City Institute.

With a global marketing and service network, Dahua Technology has established 57 branches covering the Asia Pacific, North America, South America, Europe, Africa and other regions to provide customers with

speedy and high-quality services. Dahua Technology has deployed its products, solutions, and services in 180 countries and regions, covering key industries including transportation, manufacturing, education, retail, banking & finance, energy, environmental protection, etc.

In order to vigorously innovate and continuously expand new high-growth fields, Dahua Technology attaches great importance to the cultivation of innovative businesses, and constantly seeks innovation and challenges. With accumulated experience in technological



IN ORDER TO VIGOROUSLY INNOVATE AND CONTINUOUSLY EXPAND NEW HIGH-GROWTH FIELDS, DAHUA TECHNOLOGY ATTACHES GREAT IMPORTANCE TO THE CULTIVATION OF INNOVATIVE BUSINESSES.

extend their footprints in the industry and co-partner on Dahua exhibitions or participate in Dahua partner day events; elaborate joint success stories and work out common solutions; cultivate strong and long-lasting relationships with our local sales teams and find new partners in our network across all verticals; align sales strategies and develop business in key industries, etc.

The video surveillance market is a highly competitive one. What is Dahua's USP?

Dahua Technology has always focused on smart IoT to serve the digital transformation of cities and enterprises. Through its continuous improvement and optimization of R&D and innovation, marketing and service network, supply and delivery, compliance, as well as the open and cooperative ecosystem, Dahua has gained insights into industry-specific scenarios and a profound understanding of client demands, so as to provide clients with satisfying smart IoT solutions and establish its core competitiveness.

How do you ensure the security of your products?

The cybersecurity of our products is a top priority for Dahua. We strive to develop and maintain state-of-the-art cybersecurity practices, including inputting network security into the product life cycle of all our new products and establishing our customer-facing Dahua Cybersecurity Center (DHCC) for transparent vulnerability reporting and handling.

Each year Dahua dedicates a portion of our R&D budget exclusively to cybersecurity utilizing our independent security research center, partnerships with industry-leading third-party testing agencies, and precautionary steps following industry standards. Through these efforts we strive to continually evolve our cybersecurity features.

In order to help users clearly understand the security status and capabilities of the device, the product security center will assist users to conveniently and quickly set up the right security configuration to suit the scenarios.

In addition, Dahua has its Product Security Incident Response Team (PSIRT) in place to receive, process and disclose any security vulnerability related to Dahua products and solutions. It is in compliance with ISO/IEC 30111, ISO/IEC 29147 and other industry standards. 🔑

development, strong technical foundation, comprehensive insight into customer needs and in-depth understanding of segmented industries, Dahua has established 13 innovative businesses in different fields, including Display & Control, Memory Storage, Transmission, Video Conferencing, Alarm System, Video Intercom, Access Control and more. Dahua will constantly adhere to technological innovation in order to make these innovative businesses competitive for our partners and customers.

Tell us about your partner program. What are the benefits of partnering with Dahua Technology?

Openness and Collaboration are two of Dahua Technology's core values. The Dahua ECO Partner Program (DEPP) is an open partner program tailored to enhance relationships with technology vendors in the security and IoT industries. It is accessible to all technology vendors with existing and potential business relationship with Dahua Technology.

Dahua DEPP partners can benefit from three pillars: technology, marketing and sales: Receive dedicated technical support and enhance in-depth integration; Increase interoperability with their products, solutions, services and lead innovation;

MIMECAST TO SHOWCASE MIMECAST X1 PLATFORM AT GITEX

DESIGNED TO EMPOWER ORGANISATIONS TO MITIGATE RISK AND MANAGE COMPLEXITIES WITH EASY-TO-DEPLOY CYBERSECURITY SOLUTIONS.

Mimecast, an email and collaboration security company, will showcase the Mimecast X1 Platform at GITEX

Technology Week 2022.

The widespread adoption of hybrid work environments coupled with the increased usage of digital-centric communication channels has expanded the attack surface – creating new organisational security risks for both people and data. By safeguarding email and business communications, the Mimecast X1 Platform is engineered to leverage a rich source of intelligence to learn about people and how they collaborate. These insights enable organisations to work protected by protecting their people, data, and communications.

The Mimecast X1 Platform is designed to mitigate risk across email communications – the No. 1 attack vector – and help empower organisations to secure their workplace environment wherever work happens. It serves as the foundation of the Mimecast Product Suite – built to drive

industry-leading detection capabilities, deliver reliability, resilience and scale, and transform data into insights that turn email and collaboration security into the eyes and ears of organisations worldwide.

The Mimecast X1 Platform encompasses four core innovations designed to mitigate risk and manage complexities:

- **Mimecast X1 Precision Detection:** Mimecast X1 Precision Detection is engineered to apply the latest advancements in AI and Machine Learning and enable intelligent detection of emerging and unknown threat types, while layered protection keeps users safe all the way down to the point of risk. The industry's most robust view of the email threat landscape – derived from Mimecast's inspection of 1.3 billion emails daily – powers instantaneous blocking of the vast majority of email-based threats.
- **Mimecast X1 Service Fabric:** By allowing customers to grow securely and seamlessly and uncover user insights that can accelerate detection and response, the Mimecast X1 Service Fabric provides the foundation for cloud-delivered security at scale.
- **Mimecast X1 Data Analytics:** Providing the foundation for a wide array of services and capabilities – from the discovery and analysis of new threats and accelerated product innovation to rich context for threat researchers and support for cross-correlation of data with systems beyond email – X1 Data Analytics is built with one primary



goal in mind: making information actionable for customers.

- **Mimecast Extensible Security Hooks (MESH):** MESH exposes a vast API ecosystem that supports fast, simplified integration of Mimecast with existing security investments. Hundreds of integrations to third party security solutions have been implemented, spanning SIEM, SOAR, EDR to TIP and XDR. The result is reduced complexity, lowered risk, and optimised security investments.

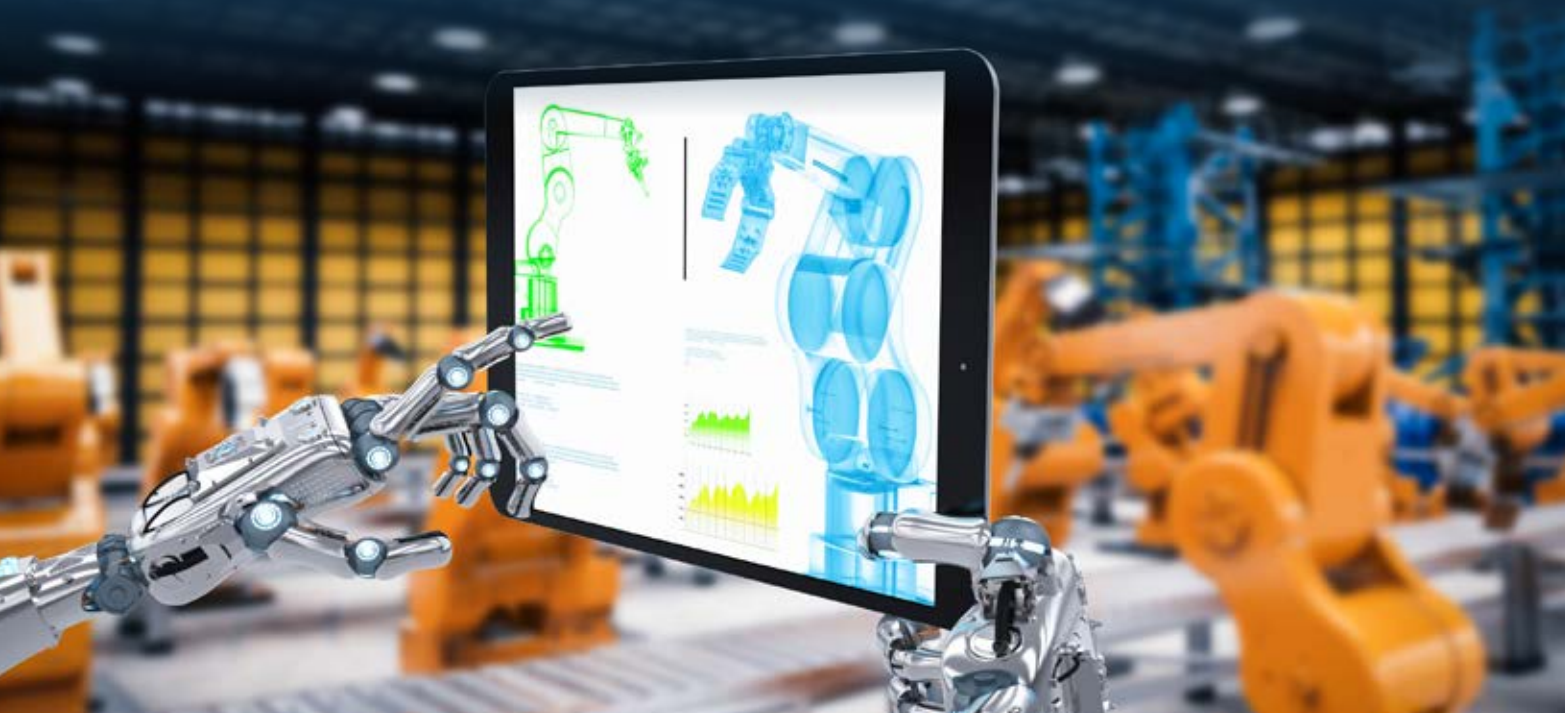
Werno Gevers, cybersecurity expert at Mimecast, said: "GITEX offers companies a great opportunity to share new solutions with the market and connect with customers, partners and other likeminded organisations. For Mimecast, it's also an opportunity to share our new vision of helping the world work protected and the importance of an integrated ecosystem. Since we're sharing a stand with our partner Netskope, we looking forward to showcase how organisations can leverage Netskope's security cloud and Mimecast's email security to provide better protection and response against a broad range of malicious actors."

Mimecast will be sharing a stand with API partner Netskope in Hall 1 - E2. 📍

**THE MIMECAST X1 PLATFORM
IS DESIGNED TO MITIGATE
RISK ACROSS EMAIL
COMMUNICATIONS – THE NO.
1 ATTACK VECTOR.**

EMBRACING OPPORTUNITIES THROUGH EMERGING TECHNOLOGIES

We help companies make the promise of digital transformation a reality.



Digital Transformation



Business Operations
Improvement



Strategy &
Transformation



Data Analytics



Governance, Risk &
Compliance



Human Capital
Consulting



Technology Consulting



Forensic Services



Transaction Services



Cyber Security Services



Financial Risk
Management



Internal Audit

Our Offices in MENA Region:

Abu Dhabi

Phone: +971.2658.4640
Fax: +971.2658.4641
Email: abudhabi@protivitiglobal.me

Bahrain

Phone: +973.1710.0050
Fax: +973.1710.0051
Email: bahrain@protivitiglobal.me

Dubai

Phone: +971.4438.0660
Fax: +971.4438.0655
Email: dubai@protivitiglobal.me

Egypt

Phone: +202.2586.4560
Email: egypt@protivitiglobal.me

Kuwait

Phone: +965.2242.6444
Fax: +965.2240.1555
Email: kuwait@protivitiglobal.me

Oman

Phone: +968.2469.9403
Fax: +968.2469.6356
Email: oman@protivitiglobal.me

Qatar

Phone: +974.4421.5300
Fax: +974.4421.5288
Email: qatar@protivitiglobal.me

Saudi Arabia

Phone: +966.11.298.7100
Fax: +966.11.217.0180
Email: saudi Arabia@protivitiglobal.me

MAKING SECURITY SEAMLESS

MOHAMMAD ISMAIL, REGIONAL DIRECTOR - MIDDLE EAST, DELINEA, TELLS SECURITY ADVISOR ME THAT AS REMOTE WORK, HYBRID IT ENVIRONMENTS, AND NEW TYPES OF APPLICATIONS AND ENDPOINTS CONTINUE TO EXPAND THE ATTACK SURFACE, THERE IS AN URGENT NEED TO BRING TOGETHER PAM CAPABILITIES THAT ADDRESS TRADITIONAL AND EMERGING USE CASES FROM ONE UNIFIED INTERFACE.



Theme of Delinea's participation

As organisations continue their digital transformations, they are faced with

increasingly sophisticated environments and more challenging requirements for securing an expanded threatscape. Legacy PAM solutions are not designed for today's hybrid environments, are too complex, and cannot solve current privilege management challenges.

Our core message to attendees at GITEX is that the opposite of complex isn't simple – it's seamless. Our mission is to provide security that's invisible to the user, while simultaneously providing IT and security teams with the control they require.

Solutions that Delinea will be showcasing at GITEX Global 2022:

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. At GITEX, we will showcase our portfolio of solutions that empower organisations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security. We offer a comprehensive and modern PAM solution portfolio that not only provides the right users just-in-time and just enough access to critical data, servers, and applications but also provides end-to-end monitoring and reporting to identify abuse of privilege and quickly thwart attacks.

Expectations and Plans for the show this year:

GITEX this year will be especially relevant to us as it will be the first edition of the show where we will participate under our new brand identity which was unveiled earlier this year following the successful merger of established Privileged Access Management (PAM) leaders Thycotic and Centrify. We are excited to have the opportunity to introduce prospects, customers, and partners to Delinea, and to our new Regional Director, Mohammad Ismail, who joined us in August year from our valued distributor partner, Shifra.

Through our engagements at the event, we want to emphasize that whether in the cloud or on-premises, Delinea provides powerful, customisable, and scalable solutions to secure organisations of any size or in any industry, no matter their PAM maturity.

Forward-looking plans:

Remote work, hybrid IT environments, and new types of applications and endpoints continue to expand the privileged account attack surface. This has created an urgent need for a holistic vision, bringing together PAM capabilities that address traditional and emerging use cases from one unified interface – what we at Delinea call Extended PAM.

As business requirements and the threat landscape has evolved, so too has our regional strategy. We are presently focused on evangelising the Middle East market on how the Extended PAM approach redefines PAM to treat all users as privileged users and address complex IT environments. Our aim is to help businesses recognise how this solution ensures scalability by treating identity as the common thread for authentication and applying policy-based authorisation controls to meet zero trust and least privilege best practices. 🛡️



Global
Cybersecurity
Forum

9-10 Nov 2022

The Ritz Carlton Riyadh
Saudi Arabia

RETHINK THE GLOBAL CYBER ORDER

JOIN US FOR THE FORUM'S 2022
EDITION, FEATURING:

5

ENGAGING THEMES

120+

SPEAKERS

4500+

ATTENDEES

30+

SESSIONS

JOIN US

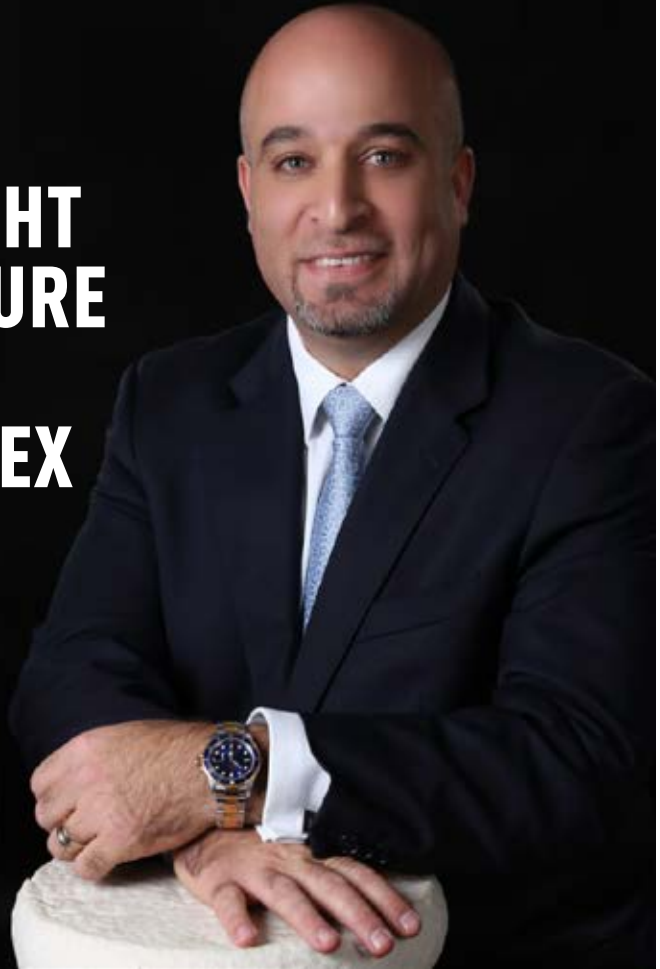


LEARN MORE ABOUT #GCF2022

globalcybersecurityforum.com

TENABLE TO HIGHLIGHT CONTINUOUS EXPOSURE MANAGEMENT CAPABILITIES AT GITEX

AT GITEX 2022, WE WANT TO HELP ORGANISATIONS APPRECIATE WHAT CONSTITUTES THE MODERN ATTACK SURFACE.



Tenable, the Cyber Exposure Management company, will exhibit at GITEX Global at the Dubai International Convention and Exhibition Centre from October 10 - 14, 2022. At the event, Tenable will showcase its powerful combination of continuous exposure management solutions for the modern attack surface that will help organisations translate technical asset, vulnerability and threat data into clear business insights and actionable intelligence.

GITEX is timely given the dramatic rise

of ransomware, nation state-sponsored threats and a flood of new vulnerabilities, which has seen cybersecurity teams under siege. This follows the dramatic adaptations businesses have made to how they operate — with cloud adoption, new applications and the increased use of personal devices and remote access tools transfiguring the corporate attack surface. For security teams, managing the plethora of technologies has been a challenge, leaving enterprises vulnerable to cyberattacks.

"When we think of traditional network

security, the goal is to fortify the perimeter to prevent threats outside of the network from getting in. However, the way we work today means this approach is no longer feasible," said Maher Jadallah, Senior Director Middle East & North Africa, Tenable. "At GITEX 2022, we want to help organisations appreciate what constitutes the modern attack surface. Our team will be on hand to help them understand how they can focus their efforts to prevent likely attacks, and accurately communicate exposure risk to their business partners to improve performance cross functionally."

Tenable will be co-exhibiting alongside AmiViz, from booth H1-A1 and Ingram Micro from booth H3-D30. The Tenable Team will be offering demonstrations of its continuous exposure management platform, including Tenable.io, Tenable.sc, Tenable.ot, Tenable.ad and Tenable Lumin. 

THE TEAM WILL BE ON HAND TO HELP BUSINESSES UNDERSTAND HOW THEY CAN FOCUS THEIR EFFORTS TO PREVENT LIKELY ATTACKS.

Solar Powered Camera

No network cable required

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

Easy installation

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

Can withstand bad weather

Prone to extreme weather such as strong wind and rainstorms.



2MP
@ 30 fps



40W



20 Ah
lithium



4G



Beaufort scale **12**



IP67



Scan to Learn More



HIKVISIONMENA



HIKVISION-MENA



HIKVISIONMENA



HIKVISIONMENA

HIKVISION

FORTINET SURPASSES 1 MILLION NETWORK SECURITY EXPERT (NSE) CERTIFICATIONS ISSUED

FORTINET CONTINUES TO EXPAND THE GLOBAL IMPACT OF ITS TRAINING AND CERTIFICATION PROGRAMS WITH THE ADDITION OF NEW COURSES IN PRIORITY CYBERSECURITY AREAS.

Fortinet, a global leader in broad, integrated and automated cybersecurity solutions, has announced it has issued more than 1 million Network Security Expert (NSE) certifications to date, further advancing its commitment to close the cybersecurity skills gap. Adding to this milestone, Fortinet continues to expand the global impact of its training and certification programs with the addition of new courses in priority cybersecurity areas, new training partners, and by expanding access to cyber training and education to empower untapped talent. Fortinet also continues to help organisations build a cyber-aware workforce through its existing Security Awareness and Training Service and through a recent initiative tied to the 2022 White House National Cyber Workforce and Education Summit, by

providing a tailored version of the service available for K-12 school districts in the U.S. free of charge.

John Maddison, EVP of Products and CMO at Fortinet said, "Fortinet has a long history of working to close the cyber skills gap and we are proud to share we recently hit a significant milestone by achieving more than 1 million Network Security Expert (NSE) certifications issued to date. Continued learning through training and certifications is a critical way to stay ahead of cyber adversaries who are constantly evolving their attack strategies and methods. This is why Fortinet's Training Institute is dedicated to offering award-winning cyber training and certifications for security professionals to upskill and advance their knowledge or for those considering reskilling. At the same time, for organisations looking to build cyber awareness in their



employees and strengthen their posture, the Fortinet Training Institute offers its Security Awareness and Training service.”

Advancing Skill Sets in Cybersecurity Professionals to Keep Up with Threats

With more than 80% of breaches being attributed to a lack of cyber skills according to a global 2022 Fortinet report, the cybersecurity skills gap continues to be a top-of-mind concern for organisations. In an effort to help close the cyber skills gap, Fortinet through its Training Advancement Agenda (TAA) and Fortinet Training Institute initiatives is focused on upskilling security professionals to stay ahead of threats with the following efforts:

- **Validating Skills and Experience with NSE Certifications:** As part of Fortinet’s progress to close the skills gap, the Fortinet Training Institute achieved the milestone of over 1 million NSE certifications issued to date. The eight-level training and certification program is designed to provide technical professionals with independent validation of their security and networking skills as well as work experience. Fortinet’s 2022 Global Skills Gap report revealed that 95 percent of leaders believe

technology-focused certifications positively impact their role and their team, while 81 percent of leaders prefer to hire people with certifications. The Fortinet Training Institute aims to provide professionals the opportunity not only to gain skills to ward off cyber threats, but also career growth opportunities, as leaders value certifications. In addition, NSE training curriculum is easily accessible to empower access to learning and is offered in instructor-lead, virtual instructor-led, and free self-paced training formats.

- **Developing Courses in Key Cybersecurity Areas Across all Industries:** The Fortinet Training Institute is continuously updating its training with content that is relevant and dynamic for the issues and challenges cyber professionals face today. For example, the OT Security curriculum, as part of NSE level 7, provides a solid understanding of how to design, implement and operate an OT security solution for critical infrastructures. Other topic areas where the Fortinet Training Institute has expanded curriculum include Zero Trust Network Access

and Secure SD-WAN, among others. Additionally, Fortinet offers low-cost labs to further advance skill sets for anyone taking technical, advanced or expert level training.

- **Leveraging Threat Intelligence from FortiGuard Labs in Curriculum:** The Fortinet Training Institute curriculum is developed by Fortinet’s world-class trainers and curriculum developers with an in-depth knowledge of industry-leading technology and the evolving threat landscape. The training curriculum is augmented with FortiGuard Labs’ threat intelligence, a global research team comprised of experienced threat hunters, researchers, analysts, engineers, and data scientists. In addition, the curriculum is designed to evolve based on the latest threat intelligence from FortiGuard Labs, ensuring that anyone taking training and pursuing certification obtains the most relevant skills and knowledge.
- **Offering Opportunities for Professionals to Upskill Through Fortinet’s Global Authorized Training Centers:** Fortinet Authorised Training Centers (ATCs) are a network of accredited training

organisations in more than 130 countries and territories around the world, teaching in 26 different languages. ATCs deliver the Fortinet Training Institute's cybersecurity training in local languages. New ATCs that have recently joined the program, extend the availability of Fortinet's training to security professionals around the world, including: Exclusive Networks (USA), Wavelink (Australia), HRP (Hungary), and DACAS (The Caribbean).

Expanding Access to Cyber Training and Empowering Untapped Talent

Fortinet is increasing access to cybersecurity training so that more people, regardless of their educational background, current career or life experience, can access cyber courses and help kickstart a career in cybersecurity. Fortinet is also empowering untapped talent pools, including women, students, veterans and more, to reskill or expand their skills for a career in cyber, helping to address the industry talent shortage. As part of this focus, Fortinet made a commitment in September of 2021 to train 1 million people in cybersecurity over 5 years between 2022-2026 and is on track to meet this through various initiatives, including:

- **Enhancing organisations' cybersecurity awareness training for all employees with the Security Awareness and Training Service:** Any company looking to further protect their security posture by advancing all their employees' cyber skill sets and knowledge can easily deploy the Fortinet Training Institute's Security Awareness and Training Service. This service introduced earlier this year is a SaaS-based offering that delivers timely awareness training on today's cybersecurity threats. It helps IT, security, and compliance leaders build a cyber-aware culture where employees recognise and avoid falling victim to cyberattacks.



- **Offering a Free Security Awareness and Training Service for K-12 School Districts in the U.S.:**

Fortinet announced that it has made its Security Awareness and Training Service available to K-12 school districts across the United States free of cost, making the training available to approximately 8 million faculty and staff. Educational institutions have seen an increase in bring your own devices (BYOD) making schools and students more vulnerable to cyber threats due to the expanding attack surface and, thus, must ensure they are securing their critical digital assets and sensitive information. With the tailored service, school districts can implement training for staff and faculty to expand their skill sets and cyber knowledge, so they don't fall victim to popular threat methods as part of the overall school cybersecurity strategies.

- **Expanding Academic Partner and Education Outreach Programs**

Partnerships: With more than 470 Authorised Academic Partners around the world across more than 90 countries and territories, the Fortinet Training Institute continues to work with education institutions

globally to help prepare the cyber workforce of the future. Among the new institutions worldwide that have joined the Academic Partner Program are: Universidad Panamericana (UP) in Mexico, Technological University of Queretaro (UTEQ) in Mexico, KLE Tech University in India, South Regional TAFE in Australia, Università di Tor Vergata of Roma in Italy, Cybersecurity Business School in France, UIB - Universitat de les Illes Balears in Spain, Polytechnic Institute of Guarda in Portugal, University West - Höskolan Väst in Sweden, South Texas College in the United States and more. As Authorised Academic Partners, these institutions are using Fortinet's award-winning technical training in their classrooms and providing students with valuable industry certifications to add to their resumes upon graduation.

Similarly, the Education Outreach Program is expanding Fortinet's reach by partnering with additional organisations who represent traditionally underrepresented groups in the high-tech sector such as women, veterans, economically disadvantaged and more. New outreach partners include Cerco IT and National Economic Education Trust (NEET). 📌

GLOBAL
DEV
SLAM

10-13 OCT 2022
DUBAI WORLD TRADE CENTRE

×

GITEX
GLOBAL

Supported by

مقر المبرمجين
coders(hq)

Featuring the inaugural



POWERING CODING INGENUITY

THE WORLD'S LARGEST MEET UP FOR
THE DEVELOPER & CODING COMMUNITY

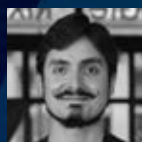
TECH PIONEERS ON STAGE



Travis Oliphant
Creator of NumPy
& Co-Founder



USA



Sebastian Ramirez Montano
Creator



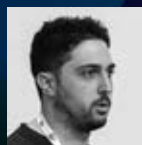
Germany



Ketan Umare
Co-Creator of Flyte,
Co-Founder & CEO



USA



Pablo Galindo Salgado
Physicist & Software Engineer
- R&D Python Infrastructure



UK

DON'T MISS OUT,
GET YOUR DELEGATE PASS



For delegate group booking, call Fahad Khalife at:

+971 4 308 6805 | globaldevslammarketing@dwtc.com

[GLOBALDEVSLAM.COM](https://globaldevslam.com)

#GLOBALDEVSLAM

Founding Partners



ORACLE



Gold Sponsor



Silver Sponsor



TRELLIX LAUNCHES ADVANCED RESEARCH CENTER

TRELLIX ADVANCED RESEARCH CENTER HAS THE CYBERSECURITY INDUSTRY'S MOST COMPREHENSIVE CHARTER AND IS AT THE FOREFRONT OF EMERGING METHODS, TRENDS AND ACTORS ACROSS THE THREAT LANDSCAPE.

Trellix, the cybersecurity company delivering the future of extended detection and response (XDR), has announced the establishment of the Trellix

Advanced Research Center to advance global threat intelligence. Comprised of hundreds of the world's most elite security analysts and researchers, the Advanced Research Center produces actionable real-time intelligence and threat indicators to help customers detect, respond and remediate the latest cybersecurity threats.

"The threat landscape is scaling in sophistication and potential for impact," said Aparna Rayasam, Chief Product Officer, Trellix. "We do this work to make our digital and physical worlds safer for everyone. With adversaries strategically investing in talent and technical know-how, the industry has a duty to study the most combative actors and their methods to innovate at a faster rate."

Trellix Advanced Research Center has the cybersecurity industry's most comprehensive charter and is at the forefront of emerging methods, trends and actors across the threat landscape. The premier partner of security operations teams across the globe, Trellix Advanced Research Center provides intelligence and cutting-edge content to security analysts while powering our leading XDR platform. Additional information can be found on



the Trellix Advanced Research Center blog and in our Threat Center.

Python Tarfile Vulnerability Highlights Software Supply Chain Complexities

In coordination with today's launch, Trellix Advanced Research Center also published its research into CVE-2007-4559, a vulnerability estimated to be present in over 350,000 open-source projects and prevalent in closed-source projects. It exists in the Python tarfile module which is a default module in any project using Python and is found extensively in frameworks created by Netflix, AWS, Intel, Facebook, Google, and applications used for machine learning, automation and docker containerisation. The vulnerability can be exploited by uploading a malicious file generated with



two or three lines of simple code and allows attackers arbitrary code execution, or control of a target device.

"When we talk about supply chain threats, we typically refer to cyber-attacks like the SolarWinds incident, however building on top of weak code-foundations can have an equally severe impact," said Christiaan Beek, Head of Adversarial & Vulnerability Research, Trellix. "This vulnerability's pervasiveness is furthered by industry tutorials and online materials propagating its incorrect usage. It's critical for developers to be educated on all layers of the technology stack to properly prevent the reintroduction of past attack surfaces."

Open-source developer tools, like Python, are necessary to advance computing and innovation, and protection from known vulnerabilities requires industry collaboration. Trellix is working to push code via GitHub pull request to protect open-source projects from the vulnerability. A free tool for developers to check if their applications are vulnerable is available on Trellix Advanced Research Center's GitHub. [i](#)

TRELLIX ADVANCED RESEARCH CENTER PROVIDES INTELLIGENCE AND CUTTING-EDGE CONTENT TO SECURITY ANALYSTS WHILE POWERING ITS LEADING XDR PLATFORM.

GITEX
GLOBAL

— NEW —
**GLOBAL
DEV
SLAM**

ai
عالم الذكاء الاصطناعي
EVERYTHING

**NORTH
STAR**
INSPIRED BY
GITEX GLOBAL
DUBAI

**Fintech
SURGE.**
فينتك سيرج

FUTURE
BLOCKCHAIN
SUMMIT
قمة مستقبل البلوك تشين

— NEW —
X V E R S E

ماركتنغ مينيا
**Marketing
Mania**

10-14 OCT 2022 DUBAI WORLD TRADE CENTRE

SHOW TIMINGS: 10 Oct - 11am to 5pm | 11 - 14 Oct - 10am to 5pm

THE WORLD'S LARGEST & MOST INFLUENTIAL TECH + STARTUP EVENT



GET YOUR
EVENT PASS



Believe the hype, it's here.
ENTER THE NEXT DIGITAL UNIVERSE

DIAMOND SPONSOR



TECHNOLOGY & DIGITAL PARTNER

TECH & DIGITAL
A NEOM COMPANY

SILVER
SPONSOR

ManageEngine
a division of Zoho Corp.

PLATINUM & LANYARD SPONSOR



CONNEXIONS
LOUNGE SPONSOR

INNOVATION
PARTNER

@ DUBAI
INTERNET
CITY

GOLD SPONSOR



MAJLIS
LOUNGE SPONSOR

midis
GROUP

GOLD SPONSOR



ATTENDEES
BADGE SPONSOR

VINFAST

TECH
NATION
PAKISTAN

The CSOC in Riyadh builds on Help AG's expertise of more than 25 years in providing world-class cyber defence to organisations in the region.

Help AG, the cybersecurity arm of e& enterprise and the Middle East's trusted security advisor, has launched a state-of-the-art Cybersecurity Operations Centre (CSOC) in Riyadh, Saudi Arabia, to provide 24/7 security monitoring and events management, along with a complete suite of locally delivered Managed Security Services (MSS), fully compliant with the local data regulations.

The CSOC in Riyadh builds on Help AG's expertise of more than 25 years in providing world-class cyber defence to organisations in the region. The launch comes at a critical time as Saudi Arabia is accelerating its digital transformation and focusing on creating a collaborative ecosystem with the ultimate goal of becoming a global investment powerhouse – a key pillar in the Kingdom's 2030 Vision.

Commenting on the launch, Stephan Berner, Chief Executive Officer at Help AG, said: "With increased digital adoption across Saudi Arabia, embedding cybersecurity in every project and process has quickly emerged as a top-of-mind moving target for organisations in the kingdom. The launch of our state-of-the-art CSOC reflects Help AG's deep commitment to supporting Saudi Arabia's vision of digital transformation. Featuring our next-generation security operations framework for enterprises and governmental entities, as well as offering flexible deployment through cloud, on-premise or a hybrid model, the CSOC in Riyadh will enable our Saudi clients to take timely action on the basis of threat intelligence feeds and through our security orchestration and automation platforms."

Fahad Al-Suhaimi, Country Director for Saudi Arabia, Help AG, said: "The launch of the Riyadh CSOC is a key milestone in Help AG's journey in Saudi Arabia which began in 2017, and reflects our dedication to providing our customers in this market with comprehensive cybersecurity services while emphasising our continued support



HELP AG LAUNCHES CYBERSECURITY OPERATIONS CENTRE IN RIYADH

for Saudisation efforts in the IT sector with a team of talented nationals.

"The launch comes as more organisations recognise the vital importance of Managed Security Services for establishing cyber resilience in the modern threat landscape. In fact, we forecast that 90% of all cybersecurity requirements will be fulfilled by a service model in three years, reflecting an industry-wide shift which we are spearheading in the region through

delivering global and advanced security services while moulding them to address regional market threats and requirements."

With 360-degree cybersecurity offerings combining organisational and technical expertise, backed by a world-class innovation ecosystem and 24/7 monitoring, Help AG's cutting-edge CSOC in Saudi Arabia offers distinct service differentiators that are fully compliant with local data regulations. 🔑

Secure Your **Digital Future**

Simple. Secure. Resilient.



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

www.raqmiyat.com

UAE | KSA | INDIA

The
Fastest
Growing
VAD

www.gulfitd.com

imperva

PingIdentity

NIAGARA
NETWORKS

Array

CATO
NETWORKS

PENTERA

CYBLE

netwrix

RESOLVE

aruba

SailPoint

CYBERARK

sealpath

corelight

Fortanix