60 MINUTES
GITEX TECHNOLOGY WEEK

CPI MEDIA GROUP
tahawultech.com @GITEX

DAY 1 AM

Show dates: 10-14 October 2022, Dubai World Trade Centre | Exhibition hours: 10am-5pm

---

The power of threat intelligence

Amir Kanaan, Managing Director for the Middle East Turkey and Africa at Kaspersky outlines how their operations have evolved, the impact of threat intelligence and the importance of SOCs.

Amir Kanaan

Tell us about Kaspersky's operations in the Middle East?
We have had our operations in the Middle East for over 15 years and are celebrating our 25th anniversary this year. Earlier this year, we opened a new office in Saudi Arabia, which adds to our ever-expanding network and is a milestone in our roadmap to protect over 400 million users

---

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.

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

---

Reimagining the digital future

du is one of the most innovative companies in the region, but a digital leader is always looking at ways to reinvent themselves. CNME Editor Mark Forker spoke to du executives Martin Tarr, Chief ICT Officer, Mohamed Al Qubaisi, Head of Products, Solutions and Digital Services, Khaled Al Mazrouei, Head of Sales and Business Development, and Marwan Bindalmook, Head of Service Management and Delivery, to learn more about the company's phenomenal transformation over the last 12 months.

Can you outline to our readers what direction the du ICT division is taking under your leadership - and what your strategy is for the next 12 months?
We have been transforming the du ICT division over the last 12 months in our efforts to make the entity a more purpose driven, customer-centric, and performance-focused organisation.

Part of that transformation has inevitably led to an evolution of our product portfolio. We have evolved

---

Modernising data protection

Kinda Baydoun, Regional Channel and Alliances Manager, Middle East and CIS at Veeam tells Reseller ME in an exclusive interview, all about data protection and how vital channel partners are for growth and success.

Kinda Baydoun

Are you participating in GITEX Global 2022? If yes, what products and solutions will you be showcasing at the event?
Yes, Veeam will be participating this year at GITEX Global. We will use the event as a platform to share our company's vision for the future of Modern Data Protection and deliver live demonstrations of Veeam Platform – the single platform for ALL workloads, whether Cloud, Virtual,

---

FortiGuarding your organisation

Alain Penel, Regional Vice President, Middle East and Turkey, Fortinet talks cybersecurity solutions, data breaches and hybrid cloud.

Alain Penel

Tell us about Fortinet's Cybersecurity Mesh Architecture (CSMA)
The expanding attack surface, increasingly sophisticated cyber threats and network security complexity create challenges for organisations in virtually every industry. A cybersecurity mesh architecture is an approach that is designed to create a collaborative ecosystem of security tools operating across the digital infrastructure. Broad reach, native integration, and advanced, artificial intelligence-based automation are the key attributes of this mesh approach. They are precisely the core attributes of the Fortinet Security Fabric.

Our Fortinet Security Fabric mesh architecture has been available for a number of years now, and over time, customers keep adding to it. Organisations

---

Empowering a new digital future

CNME Editor Mark Forker spoke to the new General Manager of Microsoft UAE, Naim Yazbeck, to learn more about the company's take on the Metaverse, the role Microsoft Cloud has played in driving new innovation, entrepreneurship and economic growth in the UAE – and its continued commitment to sustainability.

Naim Yazbeck

When I spoke with the Microsoft UAE team last year, sustainability was a key theme that featured prominently throughout the discussion. We know that Microsoft is a key partner for the UAE in terms of helping the nation achieve its national agenda objectives and outcomes. However, can you tell us about your sustainability mission - and how you're helping the UAE address issues over talent acquisition and skills shortages in the IT sector?
When it comes to sustainability, Microsoft works diligently to minimise the environmental impacts of our operations while maximising the positive impacts of our technology.

We also strive to extend those benefits across our corporate boundaries and out to the communities we serve. We are proud to be leaders in the battle to reduce carbon footprint. Having been carbon neutral since 2012, we have committed to being carbon negative by 2030.

And by 2050, we will have removed from the environment an equivalent

---

www.tahawultech.com

@tahawultech

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

Kaspersky...

and 240,000 corporate clients worldwide. With quarter of a century experience, we continue to work closely with major government entities and key industries in the region doing what we do best – protect our customer and what they value the most. To date, we have tracked activities of over 900 APT groups and collected over 1 billion malware files.

To illustrate our success in numbers, we have had steady growth in our Middle East business throughout the past years. The first half

> **Majority of all cyber-incidents are caused by human error because it takes only one click on the wrong link to let cybercriminals inside an organisation".**

of 2022 showed a 8% YoY growth and we aim to continue this streak of success in the region.

Digital transformation raises the stakes for IT security. This basically means moving your IT security strategy to a new level. How does Kaspersky's Threat Intelligence step in to help organisations stay ahead of cyberthreats?
APT groups are extremely smart, well-equipped to infiltrate any device or network to achieve their motives. They are also quick to exploit vulnerabilities in new technologies. For example, IoT has fast become a key driver of digital transformation and is crucial within today's smart city infrastructure. The Mirai botnet used enterprise-class IoT devices to launch massive DDoS attack that had dire financial and reputation consequences. APT groups also rely on smart social engineering

techniques to infiltrate their victims. The only way to stay ahead of the threats is by understanding them and preparing accordingly. For example, an airline company in the Middle East using our threat Intelligence can have access to insights on APTs targeting other airlines in the region and worldwide to understand the criminals' motives and techniques and build a cybersecurity strategy that is resilient.

Our research team is an elite group of more than 40 security experts, specialised in tracking and studying the activity of APT groups around the world. Our regional researchers are currently monitoring 29 groups in the Middle East and have issued hundreds of reports sharing expertise and insights on their operations.

Kaspersky has created a created a concept for designing IT systems with "innate" immunity, called the Cyber Immune approach. How do you implement this and ensure that IT systems are innately secure?
Whether it is industrial plants, energy facilities, cars or smart city systems, critical infrastructure cannot afford to have operations disrupted as this could affect people's lives. Although the cybersecurity industry is creating more security technologies, it is often merely playing catch-up with the attackers. So, Kaspersky decided to reinvent cybersecurity and coin the term "Cyber Immunity", a way to develop IT systems with innate protection.

Kaspersky's Cyber Immune approach is a means to create solutions that are virtually impossible to compromise and that minimise the number of potential vulnerabilities. Think of it as cybersecurity at the core, rather than being required to add additional layers of protection at a later stage.

We believe that Cyber Immunity is the future of cybersecurity. Our Cyber Immune operating system, KasperskyOS, along with a special development methodology lets developers create Cyber Immune solutions. It provides the interfaces, mechanisms and tools, while the methodology requires organisations to clearly define security objectives and the conditions in which an IT system will operate.

We've already launched products based on our Kaspersky OS. We recently launched the Kaspersky IoT Secure Gateway 1000, which is a Cyber Immune solution. Kaspersky IoT Secure Gateway 1000 is designed to serve as a secure gateway for the Internet of Things in an enterprise network.

Traditional approaches to security are no longer enough. Today, a holistic approach is necessary to stay ahead of the fast-growing threat landscape. How much of this is actually implemented in businesses in the region? What are they lacking?
Organisations are investing in a holistic cybersecurity approach. However, we are seeing a shortage of holistic cybersecurity approaches backed by strong expertise, which in the long run will always be a liability.

As compared to other global economies, our region is no exception to the dearth of talent in cybersecurity, more so in critical infrastructure industries like energy, transport, oil & gas and so on. 66% of organisations have faced significant security staffing challenges. We want to reduce this percentage, if not make it irrelevant. To do so, we work closely with various government entities and universities to train, teach and hone new and existing talent.

To combat lack of security skills, we also offer our Managed Detection and Response to organisations. Through this, organisations can get access to our experts round the clock, and can expect individually tailored ongoing detection, prioritisation, investigation and swift response to incidents.

Awareness is the first step to effective cybersecurity. How much awareness is there among organisations in the region about the growing importance of fool-proof security practices? Also, how do you view the training and capacity building capabilities available in the region?
We at Kaspersky absolutely agree that awareness is the first step to effective cybersecurity. But organisations fail to understand that awareness is not a "one-off" thing, but an ongoing process. Majority of all cyber-incidents are caused by human error because it takes only one click on the wrong link to let cybercriminals inside an organisation. A cybersafe workplace culture implemented at all levels in an organisation, from the boardroom to the workforce has the potential to defend against attacks.

We understand that people are generally not motivated to change their habits, and sometimes educational efforts turn into an empty formality. This is why using our insights, expertise and training techniques, we have designed a continuous learning approach that can help the staff play their part in the overall cyber safety of the organisation. Our Kaspersky Automated Security Awareness Platform (ASAP) takes a new approach to online

educational programs. It doesn't just provide knowledge: it builds concrete cyber-hygiene skills and practices.

In order to fight modern global cyberthreats, it's not enough to just build a Security Operations Centre (SOC) in the conventional sense – you need a SOC that is equipped with the technologies, security intelligence and knowledge that empower it to adapt to ongoing challenges. How does Kaspersky power SOCs to fight complex and complicated threats?
SOC building is a complex, costly, and long-term project. It may fail due to various reasons, given the demand for it to be intelligence-driven and have the ability to provide round-the-clock monitoring and response.

Our approach is based on hands-on experience in SOC building and operating, commercial threat hunting, APT campaigns investigations and analysing more than 380,000 new threats every day. For the SOC framework, we help organisations choose the right technologies that fit well with their business needs by understanding their processes, the nature of their business and the industry they operate in. We then move towards identifying the data most crucial for them and their customers, and ensure it is protected.

Our SOC consulting service includes the following stages:
1. Data Collection and Review: At this stage, Kaspersky assesses the existing detection and response capabilities of the SOC team, collects data needed for the framework development, and reviews the existing documents related to security operations.

2. Design: The Kaspersky team will develop complete and consistent SOC framework tailored to the customer infrastructure,

requirements and needs.

3. Build: Kaspersky can also help organisations upgrade their existing SOC from traditional to next-gen or if the situation calls for it, build one from scratch to mitigate emerging threats.

4. Implementation: The Kaspersky team in coordination with the SOC team will deploy and configure Kaspersky tools and solutions needed for SOC operation. Deployment and configuration of third-party solutions can be provided by partners or customers, if needed.

5. Talent recruitment: It is very important that the SOC team has all necessary roles, right skills and follow well-defined processes and procedures. Kaspersky helps organisations by interviewing candidates applying for IT/security positions to fit the bill.

6. Support: After the SOC starts its operation, the Kaspersky team will support its daily operation throughout the agreed time period. Kaspersky experts will support security operations in various ways, such as:
1. Using the Kaspersky Managed Detection and Response services for the most sophisticated tasks, such as incident response, digital forensics, malware analysis and security assessment
2. Consultation regarding previously designed SOC processes and procedures
3. Technical support for Kaspersky solutions
4. Red teaming exercises and maturity assessment for continuous SOC improvement

When I started my career in the IT industry more than 15 years ago, a SOC was a cybersecurity luxury and often only needed within governments. Fast forward to today, where SOCs are a main pillar of cybersecurity and play a vital role in keep an organisation one step ahead of emerging threats.

du...

our product offerings to support our customers' digital journeys by providing them with end-to-end solutions and services.

Some of these solutions and services include 5G connectivity, hybrid multi-cloud, our state-of-the-art datacenters, and cybersecurity infused with next generation SOC, IoT for Industry 4.0, plus the transformation of our clients' business applications.

I think that it's important to emphasize that the integration and deployment of these technologies are really driving business outcomes.

As you would expect with any large-scale transformation project, we have also established new best practices.

We have done this through the creation of a new digital advisory, and digital automation factory practice that will deliver a secure, flexible app development and automation capability (devsecOps) to our customers.

This will ensure that they become agile, and capable of responding to rapid business and technological changes. If we learned anything from the COVID-19 pandemic, then it was the importance of being agile.

In relation to Industry 4.0 we have also created a new practice, and as a direct result of that du is on precipice of accelerating Industrial IoT (IIoT) adoption for manufacturing and other industries in the UAE.

By leveraging our in-house best-of-breed 5G capability, we are designing and innovating use cases that take advantage of this technology to transform client organisations.

The purpose of introducing industry 4.0 technologies such as IoT in manufacturing is to drive digital transformation of production facilities and operations.

Deploying and integrating Industrial IoT technologies and solutions is aimed at revolutionising the way companies manufacture, enhance, and distribute their products.

Finally, talent retention and acquisition are a major problem for many companies, but again as part of our transformation, we have added new skills, and hired top-class ICT personnel to bring the best of du to our clients.

We all appreciate the importance of collaboration in our new digital economy, and over the next 12 months we will be looking at strengthening our alliances, and key relationships with global and local partners to help deliver economic and social benefits to the UAE.

We have witnessed a tsunami of digital transformation across the Middle East region over the last few years, but it has become evident that many businesses are struggling to meet the demands of digital transformation. How has du leveraged its knowledge and expertise as a leader in ICT to help their customers achieve their DX goals and objectives?
As businesses today are shifting the way they operate in the digital economy, they will need to further innovate by harnessing technologies that drive exceptional customer experiences, operational excellence, and data monetisation.

To achieve that then it is imperative that they embrace disruptive technologies such as the Internet of Things (IoT), Blockchain and Artificial Intelligence (AI).

We view challenges as opportunities to support enterprises' innovation end-to-end, from digital infrastructure and cybersecurity, through to innovative customer experiences and operations.

The key challenges we address include barriers to delivering customer service excellence and optimising operations across industry verticals.

In addition to this, du continues to transform services in the public sector, such as cloud migration and the increased adoption of technologies such as Blockchain and 5G.

du is focusing on networking the ICT services of the future, by supporting and implementing smart city infrastructure, facilitate visualisation and optimisation, as well as solidifying its commitment to the betterment of UAE business communities.

Throughout, du sets on utilising industry partnerships to spearhead innovation that will drive industry success for stakeholders and partners.

You are regarded by many within the industry as a thought leader in the ICT sector. However, can you tell us more about your leadership style - and in an industry that is constantly evolving, what sort of leadership skills do you need to have to drive future innovation and change in the digital economy?
A quote on leadership that has always resonated with me is from Microsoft's Satya Nadella, "Leadership is all about — creating clarity, generating energy, and driving success"

For me, it all starts with establishing a clear direction and vision for the business. Once that has been established you need to foster a culture of innovation and cross collaboration, because culture is critical.

It is also so important that you attract the best ICT talent and invest in upskilling your current employees.

I think the best way to attract top talent, and motivate existing employees to do better, is to focus on the holistic wellbeing of your employees to make sure they are all happy and healthy, and again I think this all falls under the category of 'culture'.

I think courage is also so important in business, you need to be courageous to take on a big challenge, to do what no one else will, to question the status quo, confront a difficult situation, and to never ever give up.

In addition to this, I think curiosity is a great trait, you need to question what's possible.

Finally, it's all about creativity, we need that creativity to solve the most complex problems in today's ever evolving digital world, and that is something du has in abundance.

Mohamed Al Qubaisi – Head of Products, Solutions and Digital Services, du

Can you tell us about some of the new products that du ICT will be showcasing at GITEX 2022?
We're very excited to showcase what we imagine the future is going to look like. As one of the examples at GITEX 2022, we will be demonstrating some use-cases that we have established with the government on the Metaverse.

We're really excited about our partnership with local government authorities. We are going to combine and blend our knowledge and expertise to fully reimagine government services across the UAE, which are completely focused on delivering better experiences.

What sort of impact do you believe these new Metaverse use-cases will have in the marketplace?
Everybody quite naturally is focused on data and trying to find new ways to extract value from data to make better business decisions.

Our idea is to infuse the concept of blockchain, and the Metaverse to deliver an enriched experience for those accessing government services, whether that's an investor, or someone looking for healthcare, or transportation services, and so on.

However, the question becomes how can the Metaverse and this new digital world powered by blockchain transform that process into a very simply, easy customer, or citizen experience?

Our objective is to evolve the journey for entrepreneurs accessing government services to make decisions based on data.

Through the deployment of digital twin scenarios, and simulations, we can use all that data to give that investor a better decision point on where he is going to open his business, and how his business is going to perform by analysing all the data that we currently sit on.

What we want to do is utilise the wealth of data we have at our disposal, and then present that visualisation to the investor in a unique way, which is in a digital world, rather than a physical kiosk or counter.

We want to really transform that experience for the investor, so they can imagine and see what his business is going to look like in the Metaverse before he even opens it.

Khaled Al Mazrouei – Head of Sales and Business Development, du

Can you outline to our readers the evolution of the New Business & Investment strategy and execution (go-to-market) deployed by du Business - and what key industry verticals have you been focused on?
My responsibility with du from a sales point of view is to move it from being a product-focused sales organisation to a solution-focused organisation.

Essentially, we are selling industry-focused solutions directly to the healthcare, education, manufacturing and defence and security sectors.

Our objective is to create and deliver digital solutions to solve business issues.

Take for example the healthcare sector, let's say they have an issue with practitioner's registering their licenses, that's a business problem that they have. What we do is bring solutions globally, bundle it with products we have today, such as cloud and cybersecurity, and so on, to give them a holistic digital solution for their business issues.

I don't go to them with a catalogue and say to them I have cloud and cybersecurity, and this is how much it costs. That is an old, archaic, and outdated approach, the new way of selling is all about delivering digital solutions to help customers overcome their business challenges, not their technical or technology challenges.

We are also moving from territory-focused sales to industry-focused – and that shift has worked very well in terms of best practices in large

> **We have been transforming the du ICT division over the last 12 months in our efforts to make the entity a more purpose driven, customer-centric, and performance-focused organisation."**

organisations in Canada and in America, and we expect it to yield excellent results for us as we seek to help our customers overcome their business problems.

There have been some major investments and acquisitions made in relation to the Metaverse, and many analysts have dubbed it the 'future of the internet'. What's your view on it from a sales perspective?
Sales organisations have traditionally always been revenue-focused because they have monthly targets to hit. We're moving away from that mentality to a more market-focused approach.

I believe the market needs the Metaverse, because it represents the future, and we must be prepared for it.

Blockchain was an emerging technology three years ago, and the industries that were not market-focused are now lagging today as a result.

The Metaverse is

firmly in our strategy and product roadmap, but we also must look and examine what the business cases are for the Metaverse, because creating a Metaverse just for the sake of it doesn't work, you have to use it to overcome a business problem.

For example, we're looking at digital health technologies, where medical universities can leverage the Metaverse to conduct surgical training in other countries, so the medical faculty could be located here in Dubai, but the students can be connected with surgeons in Singapore for instance, and they can collaborate together to see real-life examples of surgeries in real-time.

In summary, we are very focused on the new concept of the Metaverse, and we are working closely with our partners across all the key industry verticals to see how we can bring all the benefits of the Metaverse to life in a bid to solve real business issues.

Marwan Bindalmook – Head of Service Management and Delivery, du

Can you tell our readers what it that ultimately differentiates du from its market competition?
I believe there is several key differentiators that distinguishes du from the rest of our competitors. Firstly, we provide a one-stop-shop service for our customers, and we support them in an end-to-end capacity.

We also leverage our expertise and business acumen to really help our customers on their transformation journey. We do this by harnessing our knowledge to empower them to transform their business by migrating their legacy systems into digital infrastructure.

We are a company that has customer-centricity in its DNA, we build, transform and operate – and this is what really makes du such a unique organisation.

We know that we live in a digital economy driven by digital experiences – so it is critical for organisations to deliver first-class customer experience – with that in mind, we have a dedicated service management team who supports clients with contract fulfilment to ensure that all of our customers' needs are addressed and delivered.

Our job is to really understand our customer's pain points that are unique to them, we don't engage in a hit and run when we meet our clients, instead we invest all our energy into supporting what exactly it is that they need to resolve their business issues.

Can you tell our readers more about your du centre of excellence – and the benefits of your managed services portfolio?
We have a special subgroup within du called the TNT team (transition to transformation), and essentially what they do is assist and help customers in terms of understanding their problems, managing their internal services, and basically helping them on every step of their migration journey.

Once that end-to-end digital transformation journey of transition and transformation is completed, that's when our Centre of Excellence team comes into the picture to lead technical requirements for the customers, as well as to manage customers' partners.

Our Centre of excellence is engaged and focused on constructing this new environment – and they make sure that 24/7 monitoring and incident response is always operational.

The Centre of Excellence consists of multiple areas:

First Step: We provide managed services, 24/7 support, and skilled resources that can help any business and infrastructure development.

Second Step: We provide 360-degree support, which allows customers to focus on their core business and accelerate their competitiveness in the market.

Third Step: Our dedicated team is always on hand to ensure that all the technical requirements are met - and the primary objectives of a specific project are delivered according to the contract terms.

Fourth Step: Our team works with C-suite executives to manage key relationships – and the du Business team is proactively engaged with the client on every step of the journey, ensuring customers are satisfied.

In summary, it is our mission to work with our clients to ensure we serve them as best we can, which enables the client to focus on their core business, and they entrust us with the responsibility of resolving their challenges.

As a UAE national company, it is our goal to make sure that our clients have better opportunities to thrive and succeed in the new digital economy.

The power of predictive intelligent cybersecurity

AmiViz and Blackberry aim to showcase the potential of predictive intelligence of cybersecurity at GITEX Global 2022.

Ilyas Mohammed

AmiViz, the Middle East region's first enterprise B2B marketplace announced today a joint showcase of security solutions with BlackBerry at GITEX Global 2022. The companies boast a strong relationship, with AmiViz hosting the full portfolio of BlackBerry cybersecurity products on its online marketplace.

Ilyas Mohammed, Chief Operating Officer at AmiViz said "We are extremely pleased to align with Blackberry for GITEX this year and present its solutions, which can help businesses of all sizes in the region to strengthen their cybersecurity posture against cyberthreats".

During the five-day event, Blackberry will showcase its Cybersecurity Platform – Cylance Endpoint Security suite – which provides complete security, effectively predicting and protecting against sophisticated threats using advanced AI and machine learning. It provides a total Zero Trust solution with coverage across the full spectrum of devices, ownership models, networks, apps and people. Furthermore, it continuously authenticates users and dynamically adapts security policies to deliver a Zero Touch experience that improves security with no user interruption.

The BlackBerry Cylance Endpoint Security suite is a comprehensive Unified Endpoint Security (UES) solution that is capable of delivering complete "prevent, detect, and respond" cybersecurity to enterprises of any size, and in any industry, across the region. If enterprises from the Middle East need the extra security layer of Unified Endpoint Management (UEM), Blackberry's Cybersecurity Platform natively integrates with BlackBerry Cylance UEM, or works alongside any UEM solution from other vendors.

Mohamed Helmy, General Manager, BlackBerry, said "BlackBerry UEM is a business enabler that delivers complete, unified endpoint management and policy control for a diverse and growing fleet of devices and apps. With its single management console and trusted end-to-end security model, BlackBerry UEM is designed to help businesses to increase the productivity of their mobile workforce while ensuring the full and ongoing protection of business data".

Commenting on BlackBerry's participation at GITEX, Helmy added: "Building on our success at Gitex last year, we are excited to be back this year as a platinum sponsor with our value partner AmiViz in GITEX 2022, meeting our friends, customers, and fellow colleagues in Cybersecurity".

To learn more about the BlackBerry Cybersecurity Platform and meet the team of experts from Blackberry and AmiViz, please visit BlackBerry at AmiViz booth A1 located in Hall 1 at the Dubai World Trade Centre, Dubai, UAE.

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.

Mohammad Ismail

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 emphasise 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.

LinkShadow...

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 behavioural 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.

Tell us about LinkShadow's threat detection capabilities.

Staying 100% protected from a cyber-attack can be a far-fetched vision. However, organisation 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's 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 behavioural 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 three main modules – Insights, Behavioural Analytics and Threat Hunting

> **LinkShadow delivers a differentiated analytics solution by combining machine learning with layered forensics.**

that essentially assists security teams with:
- Network Detection and Response
- User and Entity Behaviour Analytics
- Network Threat Hunting
- CXO Dashboards and Reporting
- Threat Intel

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 that is powered 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. Thus, empowering customers 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 licensing model. Thus, making it an easy choice for organisations to conveniently adapted 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 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 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 of 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.

Fadi Sharaf

Fortinet...

need security operations that can function at machine speed to keep up with the volume, sophistication, and speed of today's cyber threats. AI and ML-powered prevention, detection, and response strategies based on a cybersecurity mesh architecture allow for much tighter integration, increased automation, as well as a more rapid, coordinated, and effective response to threats across the extended network.

With breaches becoming increasingly common, how is Fortinet's Incident Response service helping companies remediate a security event?
Response time plays a critical role in determining the severity and repercussions of a cybersecurity incident. The longer a threat goes undetected within an organisation's network, the more damage it can do and the more costly it will likely be to recover from.

FortiGuard Incident Response Services deliver critical services before/ during/after a security incident. Our experts arm your team with fast detection, investigation, containment, and return to safe operation. To remediate a security event, we make some key determinations including how the attacker got into your network; whether they are still there; their entire footprint on your network; if they have achieved more access; what is needed to scope, contain, eradicate, and repair.

FortiGuard Labs experts have decades of first-hand investigatory and response experience. With unique skills, proven

> ## Our experts arm your team with fast detection, investigation, containment, and return to safe operation".

threat intelligence, cutting edge incident response/ forensics technology, and established processes, our professionals deliver invaluable help to security teams. Examples of compromises we respond to include, but are not limited to ransomware attacks, Business Email Compromise (BEC), Advanced Persistent Threats (APTs), web application attacks.

Moreover, for the past 10 years, Fortinet's FortiGuard Labs has been a FIRST Team that collaborates with the international confederation of trusted computer incident response teams. As an international, not-for-profit organisation composed of 600+ members from over 100 countries, FIRST's membership is composed of both national CERT (Computer Emergency Response Teams) and CSIRT teams across, but not limited to, government agencies, academia, commercial enterprises, and financial corporations from a variety of industries. Together, Fortinet and FIRST have been cooperatively assisting with the managing of cybersecurity incidents and promoting incident prevention programs.

Hybrid Cloud is the latest trend. How is Fortinet stepping in to address cloud security?
According to the 2022 Cloud Security Report, most organisations are selecting either a hybrid-cloud (39%, up from 36% last year) or multi-cloud deployment approach (33%) to integrate multiple services, provide scalability, or ensure business continuity. And with most organisations choosing a hybrid or multi-cloud strategy, not surprisingly, they face increased complexity and security challenges. Lack of security skills becomes the top challenge (61%, up from 57% last year), followed by data protection, understanding how different solutions fit together, and loss of visibility and control.

With a holistic approach to security that converges networking and security as part of a security fabric, organisations can help reduce security risk and increase control over their hybrid, multi-cloud environments. A security fabric approach goes beyond traditional security models. Instead of adopting point solutions that can lead to security gaps, a security fabric approach uses open standards and protocols to integrate all security activities into a single platform. With all security routed to the same platform, organisations can more rapidly detect, investigate, and respond to threats. Additionally, if a security fabric approach leverages machine learning (ML), the system can become a self-healing security and networking system that protects devices, data, and applications across on-premises data centres and cloud services.

Microsoft...

amount of all the carbon the company has emitted since its founding in 1975.

Our strategy involves shifting to 100% renewable energy, extending our carbon fee to our supply and value chains, and investing in new carbon-reduction and removal technology by way of a US$1 billion Climate Innovation Fund.

We have sought to lead on decarbonisation by being transparent in our reporting. And through the Carbon Call initiative, we have tried to standardise this reporting for others to help them reach their own carbon goals. (Carbon Call is a collective of organisations across multiple industries that co-operates on access to underlying data and science.)

Microsoft is investing US$50 million in AI for Earth that will accelerate innovation by putting AI in the hands of those working to directly address sustainability challenges.

However, where we as Microsoft have the biggest potential to align ourselves with the UAE's visionary leadership and the country's sustainability goal is where we work with and through partners and customers. True to our mission, to 'empower every person and every organisation on the planet to achieve more,' we are partnering with many organisations in the UAE to help them advance their own zero carbon initiatives.

Through Microsoft Cloud for Sustainability and the Emissions Impact Dashboards for Azure and Microsoft 365, our customers get access to advanced tools that allow them to manage their businesses in eco-friendly ways.

Enova, a joint venture between Dubai's Majid Al Futtaim and Abu Dhabi's Veolia Environmental Services, leveraged the power of the intelligent Microsoft Cloud to save 320 million kWh of energy, 5 million cubic metres of water, and 210,000 metric tons of carbon dioxide emissions. In June last year, DEWA used Microsoft technologies to implement digital-twins, IoT, advanced cybersecurity, AI, and smart-building management solutions at its new headquarters, Al Shera'a, set to be the tallest, largest, and smartest government Net-Zero Energy Building in the world.

And throughout these efforts, we have strived to work on skilling initiatives such as the Microsoft Cloud Society, and centres of excellence like the Energy Core to ensure the talent is there to build a sustainable future.

The decision by Microsoft to launch their data centres in June 2019 was a seismic moment for the UAE. Many business leaders have said it has served as the foundation and springboard to huge digital transformation across the country. It is now 3 years since you opened your datacentres in Dubai and Abu Dhabi, so can you tell us how you have expanded these services, and can you provide us with some tangible examples of how you have really empowered organisations to achieve more?

Microsoft is proud of our cloud ecosystem's capacity to create jobs, accelerate innovation and entrepreneurship, and foment economic growth across the Middle East.

According to a recent IDC study Microsoft Cloud will generate almost US$40 billion over four years and generate close to 100,000 jobs.

IDC's "Microsoft Cloud Dividend Snapshot" report for the United Arab Emirates shows that between now and 2026, the four-year accumulated total for new revenue from the Microsoft Cloud will be US$39 billion, with 16.6% accumulated benefit emanating from its cloud data centre regions in Abu Dhabi and Dubai. This revenue will be generated by the Microsoft Cloud ecosystem, made up of Microsoft, its partners, and its cloud customers.

Microsoft and its partner ecosystem, in support of growing local businesses, will spend about US$3.4 billion in the UAE data centre regions for services and products in local economies. And the new regions will also help eliminate some of the barriers to cloud adoption within the region. The snapshot report also shows how benefits accruing to partners will continue to rise. Microsoft partners in 2023 can expect to make US$6.40 for every dollar generated by Microsoft through its UAE cloud locations. By 2026, this figure is expected to be US$8.49.

Microsoft, its partners, and its customers will add 97,150 jobs to the UAE economy, either through direct employment or through the indirect generation of jobs in other organisations. This will include an estimated 29,430 new skilled IT jobs, highlighting the ongoing need for collaboration between public and private entities on skilling programmes to ensure that qualified professionals are on hand to assume these roles.

The Microsoft Cloud has also been a significant boon to entrepreneurship. Microsoft for Startups MEA has laid the groundwork for business growth through a series of initiatives.

One example is a partnership with Abu Dhabi Investment Office on the GrowthX Accelerator programme, which bridges the gap between corporates and tech start-ups through mentoring, demonstration days, and networking opportunities.

Another example is Highway to 100 Unicorns, a virtual-conference series that connects entrepreneurs to industry experts to help them scale their enterprises. Through the trusted, versatile Microsoft Cloud, we continued our skilling efforts for the region's youth, and furthered our upskilling and reskilling initiatives for professionals.

The Microsoft Cloud Society has trained more than 300,000 IT professionals across the Middle East and Africa, and during the pandemic, as part of a global programme, we enabled more than a quarter million people in the UAE to acquire digital skills.

In three years of operations, our Abu Dhabi and Dubai facilities have empowered organisations of varying industries and scales to accelerate their digital transformation.

Those entities include Dubai Airports, DP World, Mashreq Bank, Emaar, Abu Dhabi's Department of Culture and Tourism, Dnata Travel Group, GEMS Education, and e&.

Etihad Aviation Group transformed its finance operations using Microsoft AI and modernised its payment-inspection process using Microsoft Cognitive Services. And Zand, the first digital bank in the UAE to provide both retail and corporate services, used Microsoft Azure to reimagine the secure customer and employee experience.

Our UAE cloud services adhere to Microsoft's trusted cloud principles of security, privacy, compliance, and transparency, allowing organisations to deliver engaging customer experiences while living up to their data residency, security, and local certification obligations.

Enterprise-grade performance and the robust policies, controls, and systems needed to keep your data safe are all there in the Microsoft Cloud. Also present are the means to rapidly assess, prototype and adopt the latest technologies, from AI and predictive analytics to the Internet of Things.

The Metaverse has been dubbed as the next revolution of the internet. We have already seen Microsoft make significant investments in that space, such as its acquisition of Activision Blizzard. Can you outline to our readers how you plan on helping companies and

industry verticals benefit from the Metaverse, and other mixed reality technologies?

The Metaverse is the next step in the evolution of the Internet, and as with many other technology developments, the UAE is leading the way.

Dubai has launched its very own Metaverse Strategy aimed at positioning the emirate as one of the world's top 10 metaverse economies and a hub for the global community.

Some 1,000 blockchain and metaverse companies are envisioned, along with 40,000 virtual jobs by 2030, all of which is expected to add up to US$4 billion to the emirate's GDP by 2030. The Metaverse has many potential applications across social, commercial, and industrial use cases.

Microsoft's Metaverse vision is based around an open, trust-centric platform that prioritises identity security and privacy and ensures nobody is left behind. Instead of "One Metaverse to Rule Them All", we must strive for a Metaverse of Metaverses, where identities and content easily flow between experiences, regardless of platform.

We recently launched HoloLens 2 in the UAE. We see this device as a crucial element of the Metaverse, with an abundance of applications, including in the Industrial Metaverse, where Kawasaki now uses HoloLens to build robots for its factory floors.

We developed AltspaceVR, the leading platform for live, mixed-reality experiences that allows artists, creators, businesses, and others to create virtual events more easily. Life-like avatars, spatial sound, and immersive environments deliver realistic sensations to participants.

We also expect to enable Metaverse experiences at scale through Dynamics 365 Connected Spaces, already in preview.

Connected Spaces models how people navigate and interact with almost any space – from shop floors to factory floors – and how they manage health and safety in hybrid-work environments.

Mesh for Microsoft Teams will combine communication channels to deliver a comprehensive human-presence connection that allows avatars to innovate and add value collaboratively through any device, and with no special equipment needed.

GITEX is the region's flagship IT and technology conference, and Microsoft's stand is always one that catches the eye as one of the greatest technology leaders in

the world. Can you tell us what solutions, products and partnerships you'll be making at the event?

Microsoft comes to GITEX Global 2022 as a Silver Sponsor and a DevSlam Founding Partner. DevSlam offers a series of workshops and hackathons for the region's digital experience developers.

Delegates will be able to visit the Microsoft Hub in our exhibition area, where we shall be treating them to a series of eye-opening and thought-provoking showcases.

Our industry focuses will be on smart cities, energy, utilities, and tourism, as well as on fintech, retail, education, and cybersecurity. At our stand, we shall be co-exhibiting with 26 partners housed in 13 back-to-back pods.

Perhaps our biggest GITEX 2022 focus will be our HoloLens 2 device that we recently launched in the UAE.

We see HoloLens as a key enabler for organisations' next-gen use cases and we predict it will play a significant role in a range of emerging use cases, from the Metaverse to digital twins.

HoloLens 2 enables organisations to empower workforces through Microsoft Dynamics 365 and more than 200 applications from our rich partner ecosystem, to address industry-specific use-cases.

HoloLens blends the physical and digital, allowing innovative solution designers to cross the divide between augmented reality and virtual reality.

Thousands of leading organisations around the world, in industries from manufacturing and construction to healthcare and education, are using HoloLens 2 and Azure mixed-reality services to cut costs, reduce energy consumption, and improve learning and retention, among a range of others.

Apart from our keynote address, our speaking and panel engagements include our thoughts on Web 3.0, where we will share Microsoft's vision of our shared future and how we can get there.

We shall be speaking at the Fintech Summit, exploring the many trends faced by start-ups in that space and how digital experiences have evolved, and will evolve, across the FSI sector.

We will address education stakeholders on the future of the sector and how distance learning will continue to take shape in the wake of the many changes we have seen over the past two years.

We will lay out our position on the threat landscape and the implications of the multi-cloud reality for issues such as identity, data protection, and zero trust in cybersecurity.

We will attend AI Everything to explain the

extant trends that are driving culture changes across the region in preparation for low code, no code, and the integration of smart solutions. And we will talk at DevSlam on how we drive efficiencies, security, and collaboration in development pipelines.

What other nascent technologies in addition to the Metaverse do you see driving new innovation across the Middle East in 2023?

If we reserve our projections for the technologies that will drive innovation in the region, we must look to those that are already viable.

One of the most recent is 5G. We see 5G as the foundation of a significant number of new use cases. Many IoT projects were waiting for communications technology to take this leap. The low latency and reliability of 5G makes it the ideal bedrock for an entire generation of new use cases where remote connectivity and connection speed are determining factors for viability.

This has implications for automated maintenance of pipelines, mining, agriculture, healthcare, and many, many others. It may also accelerate drone adoption for several use cases, such as retail and logistics, agricultural surveys, and public safety.

Many technologies already in service will continue to be deployed in new areas as use cases emerge. For example, there is a growing need for cybersecurity in the Metaverse if adoption is to be sustained.

Perhaps more important than emerging tech is the emerging implications of its use and how we, as a society, rise to that challenge.

Technologies such as the Metaverse and AI have the potential to do great good, but if we do not take due care in their implementation, we could propagate undesirable results that could have implications for everything from economic equality to health and safety.

Just as it is our privilege to reap the many rewards of technology, so is it our obligation to ensure those benefits accrue evenly across the fabric of society, rather than being filtered towards a select few.

In terms of brand-new technologies, quantum computing, while still in development, deserves a mention.

While many different points of view can be found on how far we are from a viable quantum computer, some speculate that the only problems that remain are ones of scalability.

This revolution has wide-ranging latency implications for everything from AI to cybersecurity (encryption in particular).

Veeam...

Physical, SaaS and Kubernetes environments. We will also look to engage and enter into high level discussions with our ecosystem of channel partners. Over the past year, Veeam has unveiled more than 30 product updates. Trade attendees visiting the Veeam stand at GITEX can expect to learn more about the following innovations among others:

- **Veeam Backup & Replication v12** – Released as the most advanced data protection solution for Cloud, Virtual, Physical, SaaS and Kubernetes workloads, Veeam Backup & Replication v11 has been downloaded by more than 850,000 users. The company has continued innovation and expansion of its expansive feature set with v12 by further hardening the capabilities customers need in today's ever-changing IT ecosystem. The new version expands the ability to reduce business risk through improved data and systems security recoverability at scale.

- **Veeam Backup for Microsoft 365 v7** – As the Microsoft 365 backup market leader, with over 11M users under paid contract, the new version will include enterprise-grade monitoring and reporting capabilities as a result of integration with Veeam ONE, helping to keep systems and infrastructure running smoothly thanks to built-in intelligence.

- **Veeam Backup for Salesforce** - Following the success of its Microsoft 365 product, the company will provide a demo of Veeam Backup for Salesforce, a much sought-after addition to Veeam's portfolio. With the ability to back up in the cloud and on-premises, the new offering eliminates the risk of losing Salesforce data and metadata.

- **Kasten K10 v5.0** – the most complete enterprise data management solution to date purpose-built for Kubernetes. This latest release is focused on delivering a comprehensive risk management strategy, streamlined CI/CD pipelines and new ecosystem advancement details that optimise and de-risk Kubernetes investments. These advancements all aim to help the expanding Kubernetes community work more efficiently and securely in cloud native applications.

What are your expectations from the event this year?
Besides networking with customers, partners and industry peers, we will present our brand and position as a global leader in modern data protection. Veeam is the tied #1 provider worldwide during 2H'21 in IDC's DR&P market. In the latest IDC Semi-annual Software Tracker, 2H'21, Veeam had the fastest revenue growth in the worldwide data replication and protection (DR&P) market among the top five vendors, all other vendors combined, and overall market average. In fact, Veeam's YoY growth was more than double its nearest named top five competitors in the market. I can attribute much of our success to the relationships we have built and fostered at the event over the years, and I expect GITEX 2022 to be no different. We expect to build a strong business pipeline by showcasing our innovations that will help customers drive business efficiency and agility, protect their data no matter where it resides, and ensure that they are well prepared for the next stage of digital transformation.

What will be your theme of participation at GITEX?
The theme of our participation will be around 'Helping Organisations tackle Ransomware, Cloud and Kubernetes Challenges with Modern Data Protection'

How have your regional strategies changed in recent months?
The Middle East findings of Veeam Data Protection Trends Report 2022 throws up some interesting statistics:
- 98% of UAE organisations and 97% of Saudi organisations experienced unexpected outages within the last 12 months.
- 86% of UAE organisations and 84% of Saudi organisations suffered ransomware attacks, making cyber-

> **We will continue to expand our eco-system but on a soft segment basis so that each partner can find a real space where they can develop their activities".**

attacks one of the single biggest causes of downtime for the second consecutive year.
- 69% of UAE organisations and 76% of Saudi Arabian organisations are already running containers in production, while 29% and 22% respectively plan to do so in the next 12 months. There is a need for data protection to keep pace with the maturation of containers.

Veeam recognises these trends, and our focus is on giving the region's businesses the tools needed to protect the vital data and information upon which their businesses depend. We work very closely with our ProPartner ecosystem to ensure that we are helping them develop the right capabilities and offerings to meet the increasingly complex needs of the end-customer. We work with our partners in a collaborative, rather than prescriptive process that provides the ideal environment for mutual success. We will continue to expand our eco-system but on a soft segment basis so that each partner can find a real space where they can develop their activities. Customers will also be able to find any competency they're looking for via our partner ecosystem that provides a rich variety of competencies.

At GITEX this year we will be announcing and promoting new partnerships and onboarding new Veeam Accredited Service Partners (VASPs)and aggregators.

How important is channel for you and how do you enable channel partners to work with you?
We attribute a great deal of our success to our channel partners. Veeam Backup for Microsoft 365 is big focus for Veeam this year, especially with the new release which provides our Microsoft 365 customers with more control and effortless recovery. That being said, we are running many initiatives with our partners, service providers, distributors and aggregators around this solution. The initiatives include hands-on training, round tables and very attractive promotions. In addition to this, we are also planning multiple initiatives within our channel ecosystem that includes our strategic alliance partners and Veeam Accredited Service Providers (VASPs). As an example, Veeam is the one of the major ISV sponsors for the Microsoft Datacentre launch event in Qatar, which is a very strategic event that will change the dynamics of the Cloud landscape in the entire Middle East region. This is key for spreading more awareness about the Veeam portfolio, especially within the enterprise segment. We can feel a great response from our partners from across all the Middle East countries - in particular, Saudi Arabia, Egypt, UAE and Qatar, where we see huge potential in the Data Protection market, and we are witnessing the fastest growth.

What is the advice that you would like to give to the channel community at GITEX?
A key area that needs attention from partners is the ability to build specific skills and knowledge around technology domains that are in line with today's digital transformation imperatives. We see that most of our partners are still adopting the traditional model, which is being a one-stop shop for all vendors. This model is no longer viable, as customers are looking for experts and advisors. Considering the huge potential in this region, partners need to invest in their staff and decide on the big bets that will ensure their company's survival and future growth.

Any other info you would like to add?
Veeam will be exhibiting from Hall 7, Booth D-20

Cloud Box brings focused IT Infrastructure to GITEX

Cloud Box Technologies to Focus on Its IT Infrastructure, Security and Cloud Solutions at GITEX.

Cloud Box Technologies (CBT), an IT services specialist in the UAE, is set to showcase its range of solutions at GITEX Global 2022. As a Titanium Partner of Dell, the company will focus on the wide range of products. It will also lay emphasis on its cybersecurity offerings which have been strengthened over the last year with best of breed global vendor partnerships. They will also highlight their inhouse infrastructure that enables them to provide customers with seamless services.

As a trusted Systems Integrator, Cloud Box Technologies has a range of services and solutions that are offered to customers across several industries

> **Digitisation stems from our ongoing efforts to understand our customers' challenges and implementing bespoke solutions to tackle their needs".**

including healthcare, banking and finance, retail, manufacturing, education, etc. They will emphasise their smart digital transformation for both the small and large enterprise and how the company is capable of addressing customers' individual needs within set budgets. The company will also highlight its specialised capabilities of being equipped to tackle on-premise digitisation, its strong NOC as well as how it is being pre-emptive in the Managed Detection and Response (MDR) service capabilities.

"Digitisation is the buzzword and Cloud Box Technologies have been working with customers to enable them to realise these goals. The transformation that we bring into customer's changing business environment stems from our ongoing efforts to understand our customers' needs and challenges and developing and implementing bespoke solutions to tackle their unique needs. Visitors to the stand at GITEX will get a glimpse on how they manage our customers' digital transformation expectations", said, Ranjith Kaippada, Managing Director, Cloud Box Technologies.

Cloud Box Technologies will be represented by the senior management team to be able to provide a better understanding of the company's offerings. They will be located at Hall 6, Stand A1.

Ranjith Kaippada

Transform your future

Today's fast-changing world demands smarter operations and a more resilient supply chain. Infor cloud solutions, with built-in industry-specific functionality, provide manufacturers and distributors with the data insights they need to not only remain competitive—but thrive.

Be future-ready.

Visit the Infor booth H7-E50 at GITEX Global, the largest technology show in the Middle East and Africa.

infor.com/mea

MZ Technologie to showcase contactless solutions at GITEX Global

From contactless elevators using holographic buttons to touchless touchscreens, solutions designed to help break the chains of virus transmission and reduce the spread of germs.

MZ Technologie, specialists in the field of the contactless, has announced that they will be showcasing their latest solutions at GITEX Global.

"We are delighted to be exhibiting at GITEX Global this year and introducing our contactless solutions to the GCC region", said Jonathan Zerad, Chief Technology Officer and Co-Founder, MZ Technologie.

Headquartered in Gennevilliers, France, MZ Technologie offers a wide range of contactless solutions including the popular HOLOBOX which can be used to control elevators using a hologram. The solution can also be implemented to retrofit existing elevators, making it very easy to install.

Furthermore, HOLOSTOP, a touchless stop button that is used in public transport such as buses, eliminates the need for customers to physically touch the stop button. HOLOSTOP was developed using patented holographic technology.

Touchless touchscreens also known as contactless display solutions, HOLOKIOSK, is the latest addition to MZ Technologie's range of contactless solutions and

> ❞ We can retrofit any existing touchscreens into contactless display screens".

will also be on display for visitors to experience at GITEX Global.

"We can retrofit any existing touchscreens into contactless display screens. These are ideal for the rapidly growing in popularity self-checkout counters at retail outlets, transport hubs (rail, air) across the region, for example. They are also great for fast-food chains that look to offer their customers the option of skipping the queues and ordering through touchscreen kiosks at their outlets", added Zerad.

MZ Technologie's contactless solutions are also suitable for self-service kiosks, vending machines as well as ATMs. The contactless solutions are designed to help break the chains of virus transmissions and reduce the spread of germs.

In addition, MZ Technologie recently set up a joint venture and opened an office in Dubai to serve the Middle East market in partnership with a leading development firm.

Visit MZ Technologie at Stand H2-C25 at GITEX Global 2022 and experience the feeling of touching the untouchable!

The right kind of skill

Chris Dale, Principal Instructor at SANS Institute, on Cyber Deception, Cybersecurity, the threat landscape and more.

Chris Dale

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

> ❞ The modern-day attacker is educated, trained and well capable of not being restricted by today's security controls".

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 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 overflooded 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?

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.

Gopan Sivasankara

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 Value. 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, 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.

What has the last one year been like for Secureworks?

In the channel space, we signed up with Redington 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.

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.

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

> **For us, service is our DNA and we've been doing this for a really long time, so we have a clear advantage".**

> **GITEX will give us the perfect opportunity to create awareness about what XDR actually is".**

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 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. 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.

Security goes autonomous with SentinelOne

SentinelOne to Highlight Autonomous XDR Cybersecurity Platform and Identity Protection at GITEX Global 2022.

Tamer Odeh

Ranjith Kaippada

SentinelOne, an autonomous cybersecurity platform company, plans to showcase its autonomous extended detection and response (XDR) platform, and identity and credential protection solution at GITEX Global 2022, the region's largest technology exhibition. The company will also engage with channel players in key Middle East and Africa markets as part of its aspirations to expand further in the region, as the appetite for technology grows.

Joining GITEX Global 2022's extensive conference and workshop agenda, Tamer Odeh, Regional Sales Director at SentinelOne will give a presentation on 'The Importance of Identity Security Modernisation' on the first day of the event.

"GITEX Global has evolved from its original concept in step with the market and, as a result, it has maintained its position as the Middle East's key ICT exhibition. We are excited to be part of the event this year and plan to showcase our Singularity XDR and Singularity for Identity autonomous cybersecurity solutions. These solutions offer enterprises autonomous, comprehensive and responsive protection, which is absolutely vital given the rapidly evolving global threat landscape and the potential damage a security breach can cause", said Tamer Odeh, Regional Sales Director, SentinelOne.

Annual spending on digital transformation across the Middle East, Turkey and Africa is set to top $58 billion, as regional governments and organisations increasingly look to technology to find new efficiencies and respond

> **These solutions offer autonomous, comprehensive and responsive protection, which is vital given the rapidly evolving global threat landscape"**

to changing demands and new challenges. While digital transformation can certainly make a difference, the downside is governments and businesses then become potential targets for a variety of global threat actors. As a result, the need for effective cybersecurity is at an all-time high.

Cybersecurity solutions must be able to see across every corner of the enterprise, offer rapid and efficient protection across the organisation, and offer an automated response across the connected security ecosystem. SentinelOne's Singularity XDR was designed to respond to these requirements in full; it can autonomously supercharge, fortify, automate and extend protection from the endpoint to beyond, with unfettered visibility, proven protection, and industry leading responsiveness.

The XDR solution was built to be better, faster and autonomous, and is a comprehensively better approach to cybersecurity when compared to traditional approaches. Singularity XDR is also designed with the security analyst experience in mind and empowers users with richer data, smarter workflows, and powerful tools at every step of the threat lifecycle.

'Identity' cybersecurity has also grown in importance over the years since identity-based infrastructure has become a core function in terms of scaling business. Due to this, this surface has become a primary attack vector for global threat actors, with weaknesses and misuse of Active Directory playing a significant part in the most disruptive ransomware attacks committed in recent times. It's therefore vital that organisations take a deliberate, more holistic approach to secure their identity layer.

This is where Singularity for Identity comes into play. The solution is designed to: prevent attack opportunities by closing the gaps in Active Directory and Azure AD that attackers frequently exploit; prevent attack progression by finding and misdirecting covert actors aiming to steal credentials; build resilience by ascertaining insights and intelligence from attempted attacks to prevent repeated compromises.

Senior executives and cybersecurity experts from SentinelOne will be at stand C55 in Hall 1 to meet with customers and partners throughout the duration of GITEX Global 2022.

Dahua to address security and signage at GITEX

Dahua's participation at GITEX Global 2022 affirms the company's commitment to the region and its partners in the security and display solutions market

Dahua Technology, the world-leading video-centric smart IoT solution and service provider, today announced its participation at GITEX Global 2022, the Middle East's premier technology exhibition. The company will showcase its full range of security solutions and highlight its latest immersive LED Screen at the event.

Committed to its mission of enabling a safer society and smarter living, Dahua Technology offers innovative end-to-end security solutions, systems, and services to create value for city operations, corporate management, and consumers. The company works across multiple verticals, providing diverse security solutions to transportation, banking & finance, building and critical Infrastructure sectors. Their powerful, proprietary R&D develops software and customizes functions that cater to specific customer requirements.

In addition to their smart CCTV solutions, Dahua also manufactures LED and LCD screens in partnership with Rainbow LED in the UAE, expanding the company's offerings to a much wider range of products.

"GITEX Global is an important platform for Dahua Technology to display our full suite of reliable and comprehensive solutions and engage with some of the industry's biggest business innovators and executives, on a regional and international scale", said Brant Shen, General manager, UAE, Oman, Yemen at Dahua Technology. "Our presence at GITEX affirms our commitment to the region and allows us the opportunity to establish strategic partnerships that will expand Dahua's presence in a very relevant market".

"Beyond our line-up of security products, we are also spotlighting our immersive LED screen that gives viewers the impression that they

are within the scene. This technology is widely used in China, in the TV and film production industry, and we are excited to bring it to the region's most-anticipated technology exhibition this year", Shen added.

Dahua's newest immersive LED display solution will be the centrepiece of the booth. Composed of LED screens on three sides and controlled by a special LED control system, the solution allows visitors to have a deeply immersive experience with Dahua's latest technology.

Other products onsite will include Dahua's glass-

> **Beyond our line-up of security products, we are also spotlighting our immersive LED screen that gives viewers the impression that they are within the scene".**

free 3D LED display, a LCD digital touch signage kiosk powered by Android with a central management system called Dahua MPS, Dahua's new interactive whiteboard. Compatible with both Zoom and Microsoft

Teams' conference software, the Smart Interactive Whiteboard comes with a 4K camera with an ultra-wide FOV that supports basic file sharing, wireless screen sharing, reverse control and screen grouping among a

host of other rich features. Rounding off their extensive line-up of solutions is Dahua's multi-platform, high-definition video conference system with built-in support for directional audio, making it the perfect system for conferencing.

Dahua Technology will be at Stand H4-D1 in Hall 4. Product experts and senior executives from the company will be available to interact with visitors during the exhibition and guide them through Dahua's entire catalogue of video surveillance devices, as well as its smart IoT and digital signage solutions.

Managing the hybrid multi cloud

Toufic Derbass, Managing Director, Micro Focus, tells Anita Joseph about the company's participation at GITEX and the Hybrid Cloud Management X platform.

Toufic Derbass

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

> **Based on AI, HCMX will provide smart insights around reserved instance management to help you optimise usage & spend on public clouds.**

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.

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

A10 Networks announces Harmony Controller as-a-Serviceas-a-Service

The A10 Harmony Controller provides centralised management and analytics for A10 secure application services.

Amr Alashaal

Network admins for enterprises and service providers all know the pain of growth and change. Rapid or unexpected growth in users, subscribers and traffic; migration from centralised data centres to edge deployments, cloud, multi-cloud or hybrid cloud environments; and the pandemic-inspired shift to distributed and suburban/home-based applications means network administrators must continually scramble to ensure capacity is correctly and efficiently deployed to meet demand.

For the critical functions that A10 provides, including Thunder Application Delivery Controller (ADC), Thunder Convergent Firewall (CFW) and Thunder Carrier-grade Networking (CGN), customers are managing their Thunder appliances or virtual machines throughout this massive change using A10 Harmony Controller. The A10 Harmony Controller provides centralised management and analytics for A10 secure application services including A10 Thunder ADC, SSLi, CFW, and CGN in multi-cloud environments for application configuration and policy enforcement. It is available on self-managed (on-premises/cloud) and as-a-service.

Harmony Controller as-a-service has key advantages over self-managed systems, providing organisations a centralised management interface for installation, configuration, monitoring and troubleshooting of physical and virtual devices wherever they are deployed. Adding or changing Thunder devices used to require manually intensive processes for installation, licensing, registration of devices. Harmony Controller as-a-service makes those processes simple and easy to use. The service is operated by A10 to ensure its security and availability.

> **With the Harmony Controller, organisations can efficiently automate deployment and operations of application services".**

The service creates simpler elastic capacity with a management interface that automatically scales as the system grows, supporting millions of users and thousands of devices.

Harmony Controller as-a-service, Release 5.4, includes the following enhancements:

Stronger Security with Multi-Factor-Authentication (MFA)
Now, administrators can enable MFA for all the users in the account. MFA is available when the users are authenticated locally in Harmony Controller. Users need to install the Google Authenticator app on their mobile devices for a one-time set up of MFA. While users can postpone set-up, the administrator can set an enforcement deadline. The device communicator role is created for users who use Harmony Controller to register Thunder devices.

Local Authorisation after Remote Authentication
Now, users can authenticate on the remote servers, such as LDAP, TACACS +, or RADIUS, and authorise locally in Harmony Controller. The user privileges and access information are stored in Harmony Controller.

Flexible Device Configuration Backup
Now, users can schedule periodic device configuration backups with precise time-zone and frequency.

"With the Harmony Controller, organisations can efficiently automate deployment and operations of application services, increase operational efficiency and agility, enhance end-user experiences and reduce TCO, simplify the management of distributed application services to dramatically shorten troubleshooting times, receive alerts on performance or security anomalies, improve capacity planning and optimise IT infrastructure and cloud environments", said Amr Alashaal, Regional Vice President - Middle East at A10 Networks.

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.

Joe El Khoury

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 centre. 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 Centre, 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.

Leading the digital future

Abu Dhabi Government showcases 100 digital initiatives at GITEX Global 2022 with the participation of more than 30 government and academic entities

The Abu Dhabi Government officially kicked off its participation at GITEX Global 2022, which is being held from 10 to 14 October at the Dubai World Trade Centre.

In its eleventh year of participation, and under the theme of 'Leading the Digital Future', the Abu Dhabi Government is showcasing more than 100 innovative digital initiatives and projects in the field of digital transformation, all of which aim to create a unique experience for visitors by providing a unified platform that includes all government entities in Abu Dhabi.

More than 30 government and academic entities are present at the Abu Dhabi Government Pavilion, showcasing their latest digital innovative projects, initiatives and applications that aim to enhance the quality of life for the community in Abu Dhabi and support the digital transformation journey of the Emirate.

The participation of the Abu Dhabi Government at GITEX Global 2022 comes under the supervision of the Higher Committee of Digital Government in Abu Dhabi as part of its efforts to implement a governance framework across the Abu Dhabi government and make a fundamental change in the concept of government services, moving towards a digital future. It comes in line with efforts to enable an integrated digital government based on innovation and creativity to serve all members of society in the Emirate of Abu Dhabi while strengthening partnerships between government entities and the private sector.

GITEX Global 2022 offers the Abu Dhabi Government an opportunity to showcase the initiatives of government entities that were launched within the key pillars of the Abu Dhabi digital agenda, which includes government services, digital government solutions, data and artificial intelligence, cybersecurity, and digital ecosystem enablement.

His Excellency Ali Rashid Al Ketbi, Chairman of the Department of Government Support - Abu Dhabi, said: "The importance of GITEX Global 2022 lies in it being a global platform to enhance strategic partnerships between public and private sectors, explore new opportunities for meaningful cooperation with academia and major global technology companies to support Abu Dhabi's digital agenda. GITEX is a great opportunity to exchange experiences and share knowledge about emerging technologies and global initiatives, thus contributing to accelerating digital transformation in the Emirate of Abu Dhabi".

H.E. Al Ketbi added: "With its participation at GITEX Global 2022, the Abu Dhabi Government aims to showcase the achievements of the emirate in the areas of digital transformation and how we have built on those achievements, the latest of which was the transfer of all Abu Dhabi government services to the Abu Dhabi unified government services ecosystem TAMM. Through TAMM, government services were transformed to become 100% digital services, allowing the community in Abu Dhabi to easily access all government services in the Emirate and achieve their transactions smoothly and quickly".

His Excellency Dr. Mohamed Abdel Hamid Al Askar, Director General of the Abu Dhabi Digital Authority, said: "We are pleased to organise the Abu Dhabi Government Pavilion at this year's event, enabling Abu Dhabi Government entities to showcase their new digital initiatives, explore innovative ideas, and adopt digital technologies that help them advance and succeed in the field of digital transformation".

H.E. Al Askar stressed the importance of the pavilion as a platform to enhance cooperation and partnership between government entities that participate under one umbrella and unite with one goal – to enhance the quality of life for the community and achieve happiness for all residents of Abu Dhabi.

The Abu Dhabi Government Pavilion will showcase the latest projects and digital transformation initiatives that aim to improve the quality of life in the Emirate and highlight the important role that government entities play in developing fast, effective, and proactive digital government solutions that support enhancing the efficiency of government performance and contribute to enriching the customer experience.

During GITEX Global 2022, the Abu Dhabi government pavilion will also host a series of events, including a 'Capture the Flag' competition, which is one of the most known cybersecurity competitions in the world. The 'ethical hacking' competition aims to enhance the skills of 'ethical hackers', a group of cybersecurity researchers who work to penetrate websites, apps and computer networks to test their security levels and anticipate hacking attacks that companies and government entities could be exposed to.

Throughout GITEX Global 2022, the Abu Dhabi Government Pavilion will host a series of events, including the launch of innovative digital initiatives as well as the signing of agreements and MoUs to strengthen strategic public-private partnerships, facilitate the digital transformation process and secure important investment opportunities for private sector companies.

It is worth noting that more than 30 government entities are gathering under one umbrella to present innovative digital solutions and technologies utilised to enhance government performance to ensure Abu Dhabi's leadership in this field, namely: Department of Community Development, Department of Municipalities and Transport, Department of Health, Abu Dhabi Department of Energy, Department of Economic Development, Department of Education and Knowledge, Department of Culture and Tourism, Department of Finance, General Directorate of Abu Dhabi Police, Department of Government Support, Abu Dhabi Accountability Authority, Abu Dhabi Judicial Department, Abu Dhabi Agriculture and Food Safety Authority, General Administration of Customs, Environment Agency-Abu Dhabi, Abu Dhabi Quality & Conformity Council, Human Resources Authority, Abu Dhabi Civil Defence Authority, Abu Dhabi Digital Authority, Abu Dhabi School of Government, Zayed Higher Organisation for People of Determination, Social Care and Minors Affairs Foundation, Family Development Foundation, Authority of Social Contribution - Ma'an, Abu Dhabi Sports Council, Abu Dhabi Investment Office, Abu Dhabi Chamber, Abu Dhabi Public Health Centre, Statistics Centre - Abu Dhabi, Abu Dhabi Centre for Technical and Vocational Education and Training (ACTVET), Khalifa University, and Abu Dhabi Youth Council.

> **GITEX is a great opportunity to exchange experiences and share knowledge about emerging technologies and global initiatives, thus contributing to accelerating digital transformation in the Emirate of Abu Dhabi".**

نقـــود
المستقبل الرقمي
LEADING THE DIGITAL FUTURE

Radware launches cloud security centre

Radware Responds to regional demand for low latency performance and complies with offshore data routing requirements.

Haim Zelikovsky

Radware, a leading provider of cyber security and application delivery solutions, has announced the launch of a new cloud security centre 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 Radware's existing cloud security network. Today, the network includes over 10Tbps of mitigation capacity across more than 50 security centres located around the globe.

> **The launch of the centre 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".**

"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 centre 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".

Swimlane to showcase low-code security automation at GITEX

Company to highlight Swimlane Turbine at top Middle East tech event; Swimlane Co-founder Cody Cornell in attendance.

Ashraf Sheet

Swimlane, the low-code security automation company, announced its participation at GITEX Global 2022. The company plans to showcase its innovative cloud-scale, low-code security automation platform at the Middle East's largest technology exhibition. Swimlane Turbine is a breakthrough in low-code security automation, capturing hard-to-reach telemetry and expanding actionability beyond closed extended detection and response (XDR) ecosystems.

Swimlane co-founder and chief strategy officer Cody Cornell will be in attendance with other Swimlane executives at the event to showcase the platform's capabilities. The company will be exhibiting in both the Evanssion booth at H3-MR#2 and Amiviz booth at H1-A1.

"As threat surfaces expand and present new headaches for security professionals to grapple with, it is absolutely vital for companies to stay ahead of the threat by deploying flexible, low-code automation", said Ashraf Sheet, Vice President of Middle East, Turkey and Africa (META) for Swimlane. "As a world leader in cloud-scale, low-code security automation for companies across several verticals, Swimlane is committed to preventing breaches and enabling continuous compliance with a next-generation security automation solution that functions as a system of record for all security operations".

"As part of our Middle East, Turkey and Africa expansion plans, we

> **This will help strengthen our channel network and reach by engaging with potential partners from different countries".**

believe GITEX is the perfect platform to showcase our cutting-edge security automation platform to a huge regional audience looking for the latest technologies. This will help strengthen our channel network and reach by engaging with potential partners from different countries", Sheet added.

At GITEX, Swimlane plans to demonstrate how low-code automation can help organisations overcome security talent shortages, unify complex environments and processes, accelerate responses as attack surfaces grow, and can quantify the value of security to business stakeholders. Swimlane Turbine is different from traditional security orchestration, automation and response (SOAR) platforms that are notoriously complex and used exclusively to automate basic security operations centre (SOC) workflows such as security information and event management (SIEM) alert triage, phishing, and threat intelligence.

By combining human and machine data into actionable intelligence that security professionals can seamlessly leverage, Swimlane Turbine multiplies the capabilities of an organisation's security teams and improves ROI, mean time to detect/discover (MTTD) and mean time to repair (MTTR). The solution unlocks the true promise of XDR with low-code automation that unifies visibility and actionability at the point of inception.

Swimlane has established itself as a market leader in providing security automation that is approachable and scalable for banking, insurance & finance, healthcare, energy & utilities (and other critical infrastructure), federal government, education, MSSPs & MSPs, and retailers. Swimlane is currently the largest and fastest-growing pure-play security automation company and the company recently raised a $70m USD growth round of additional financing.

Sheet added, "Security teams need a platform that is flexible and powerful enough to automate any security process, including unique use cases that go beyond what's typically expected within the SOC. Swimlane is the only solution to address the toughest automation challenges both inside and outside the SOC. Through automation, one of Swimlane's Fortune 100 customers has saved $160,000 monthly by automating 3,700 hours of work. Apart from the significant financial savings, the automation reduces staff burnout and helps maintain talent and institutional knowledge".

Trellix announces launch of new partner program

Launching in early 2023, Trellix Xtend is designed to put the partner first.

Trellix, the cybersecurity company delivering the future of extended detection and response (XDR), has announced Trellix Xtend, a new partner program designed to increase profitability, engagement, and growth across its global partner ecosystem. Trellix also announced new technology integrations to Trellix XDR through the Security Innovation Alliance, a program simplifying the development of inter-operable security products for complex customer environments.

"Our unified partner program, Xtend, continues to reinforce our priority as a channel-first business", said Britt Norwood, SVP, Global Channels & Commercial, Trellix. "We co-developed the Xtend program with our partners to create the right business model for deploying Trellix XDR. Partners can count on Trellix to help drive profitability for our partners and reward partner value".

Xtend Partner Program Launching in early 2023, Trellix Xtend is designed to put the partner first. Able to be tailored to each partner's business model and target market, the program delivers stronger customer outcomes.

Key elements of the program include:

- Partner Enablement: delivering a training curriculum that supports partners from first-sale to first-install of the Trellix XDR platform.
- Demand Creation: using differentiated sales plays to accelerate customer engagement, increase deal registration, and build sales pipeline.
- Partner Support: providing a premium post-sale experience including 24/7 support and resources, enabling trusted advisor relationships with Trellix XDR customers.
- Professional Services: featuring playbooks enabling partners to build managed services and incident response offerings, leveraging Trellix intellectual property, and apply threat intelligence from Trellix Advanced Research Centre.

New Members Join Security Innovation Alliance

Trellix expands the reach of its open platform with the addition of ten technology partners. These include an exciting partnership with Tenable, enabling a risk-based view of a customer's entire attack surface. The Trellix XDR risk score of an asset is automatically updated when vulnerabilities are shared from Tenable.io. This allows security analysts to quickly determine if a threat corresponds to a high-risk asset and enables them to respond faster via curated playbooks and orchestration.

In addition to Tenable, Trellix welcomes Lineaje, Arista Networks, Keysight Ixia, Elevate Security, Sumo Logic, SecureX. ai, Okta, GreyNoise, and CPacketNetworks to the Trellix Security Innovation Alliance (SIA). These new additions bring the ecosystem to over 800 partners integrated with Trellix XDR.

> " **Trellix expands the reach of its open platform with the addition of ten technology partners".**

Britt Norwood

The future of printing

Simon Hill, Managing Director for EMEA and APAC at Vasion on the future of work and the hybrid workplace, and on the company's participation at GITEX.

Simon Hill

What products and solutions will you be showcasing at Gitex Global 2022?
Vasion will be bringing PrinterLogic, the world leader in serverless printing infrastructure, to GITEX Global 2022.

PrinterLogic supports the future of work and the hybrid workplace. Customers can confidently and securely ensure their organisation can deliver best in class serverless print management, wherever work happens.

The elimination of the physical infrastructure is a critical step in an organisation's digital transformation journey. Print servers cost a lot of money and time relating to provisioning, licensing, cooling and powering, physical security, on-going management and maintenance including upgrades, virus scans etc. PrinterLogic modernises enterprise print management by eliminating all print servers and delivering a highly available Serverless Printing Infrastructure, thereby eliminating all these costs.

By moving from print servers to a cloud-native solution like PrinterLogic, companies significantly reduce the pains associated with deployment (no more scripting or GPOs), ongoing support (customers report 60-90% less print related IT support calls) and significantly lower resolution times. They also eliminate the security vulnerability of print servers - PrintNightmare.

With the centrally managed Direct IP printing platform delivered as a SaaS application, enterprises can empower end users with mobile printing, secure release printing, and many advanced features that legacy print management applications can't provide.

What do you hope to achieve from your participation at the event this year?
The Middle East and Africa market is a high potential growth market for our company. With GITEX being the biggest regional technology event, it is the perfect platform for us to expose our brand and capabilities and enter into high level discussions with customers and the channel in order to gain insights that will help us tailor our offerings to the needs of the market.

We are also looking to strengthen our channel ecosystem by signing new partners that share our strategic vision and can help us penetrate the market. Channel partners have a distinct advantage working with PrinterLogic. The print management software market is worth circa $650m worldwide and this is all driven by Managed Print Service (MPS) contracts. However, only around 40% of print is covered by MPS. The potential of the market is closer to $1.6bn. As organisations move to cloud-native print management they will want a solution that manages all their printers, and this is what we do best.

> " **By moving from print servers to a cloud-native solution companies significantly reduce the pains associated with deployment, ongoing support and significantly lower resolution times".**

What will be your theme of participation at GITEX?
The theme of our participation is around helping organisations eliminate print servers with the company's next generation cloud-native print management solution and eliminate the PrintNightmare security vulnerability.

Where can trade visitors find you at GITEX?
PrinterLogic will be exhibiting from stand number H4-62.

GENESYS™

GITEX GLOBAL X **Ai** EVERYTHING X **GLOBAL DEV SLAM**

10-14 OCT 2022 · 10-13 OCT
DUBAI WORLD TRADE CENTRE

Meet team Genesys and our partners IST Networks, Fourth Dimension Systems, CCR Group, HADEF, Al-Futtaim, Servion and Uniphore at GITEX Global 2022, **stand Z3-B35**.

Visit our Genesys demo stations Experience as a Service, CX Your Way, Rich Actionable Insights, Customer Journey Analytics and Frictionless Conversational AI and learn more about our innovative CX solutions in the Cloud, how AI can impact your customer journey, how to achieve the best personalized digital customer engagement and much more about next level customer experience solutions.

We are looking forward to welcoming you at GITEX 2022 in Dubai!

CONNECT WITH YOUR CUSTOMERS THROUGH EMPATHY

www.genesys.com