Commvault signs agreement with CSC UAE to strengthen national data protection

Commvault has signed a Memorandum of Understanding with the UAE Cyber Security Council at GITEX Technology Week 2023 in Dubai.

Commvault, a global enterprise leader in data management across on-premises, cloud, and SaaS environments, has signed a Memorandum of Understanding (MOU) with the UAE Cyber Security Council at GITEX Technology Week 2023 in Dubai.

The UAE Cyber Security Council was formed in 2020 by the Cabinet of the UAE to support the UAE’s ongoing commitment to safer digital transformation. The Council is tasked with creating and developing regulatory and legal frameworks that focus on cybersecurity and cybercrime, as well as securing present and upcoming technologies in the region, all in the name of improving the country’s cybersecurity outlook.

Masdar City and Huawei join forces to accelerate net zero

Masdar City and Huawei signed an MOU at GITEX to power knowledge-sharing, enhance information systems, promote carbon-conscious information and communication systems, and promote Huawei’s Net Zero Campus Framework.

Masdar City, a ground-breaking sustainable urban community in Abu Dhabi, and Huawei, a leading global provider of information and communications technology infrastructure, have joined forces through a Memorandum of Understanding that will help power the UAE’s journey to net zero. The agreement was signed on October 17 at GITEX Global 2023 by key Masdar City and Huawei leaders, that will lead to knowledge-sharing and capacity-building in net zero development, help reduce the carbon footprint of Masdar City’s information and communications technology (ICT) infrastructure, and accelerate sustainability efforts.

Sophos anticipates business challenges for the year ahead

Harish Chib, VP, Sales - Emerging at Sophos discusses the biggest challenges businesses are facing and the key technologies driving innovation.

Resecurity introduces digital identity protection in UAE

Resecurity is dedicated to safeguarding citizens and businesses in the UAE from cyber threats.

Pure Storage Simplifies Data Resilience and Enables an Enhanced Service Operations

New Disaster Recovery as-a-Service solution and scalable AI-powered management capabilities support secure, scalable, and smart enterprise business operations.

End user, Pure Storage. Digital Experience Business Unit, Pure Storage.

Industry Significance:
The rate of devastating ransomware attacks and the increasing frequency of natural disasters are upping business continuity concerns often each day. While many organisations recognize the importance of a disaster recovery (DR) plan, current DR solutions on the market are complex, expensive, and disruptive. Likewise, the current energy crisis, new environmental
CYBERSECURITY FOR ALL.

All threats, all businesses, all people.

Get fierce defenses for a world of complex threats.

Barracuda.com

Barracuda will be at GITEX Global 2023 Booth: H24 - C50
The collaboration will help protect UAE data and support government and private sectors with their continued digital transformation journeys. Commvault will support the UAE Cyber Security Council across cloud, on premise and off premise workloads, whilst providing Risk Visibility on data protection. Commvault’s team of global experts will also offer Ransomware recovery services, as well as proactive data security through Commvault’s industry leading solutions. The agreement will help raise awareness of the dangers of cyber crimes and outline best practices to ensure greater defence against data threats across the region.

HE Dr. Mohammed Al Kuwaiti, Head of the Cyber Security Council of the United Arab Emirates Government said that the cooperation with Commvault, the leading global company in the field of data management across local, cloud and hybrid environments, would within the framework of the Council’s keenness to enhance cyber security awareness culture in work places. In cyber security awareness enhances ways to confront cyber challenges and protect zero carbon cities and campuses of the future will become a benchmark for how carbon-conscious ICT to provide decarbonisation.

This new partnership will be a powerful enabler for decarbonisation.

We are actively working with both government and private sector organisations to help guarantee greater data protection and ensure enhanced sustainability, productivity and flexibility with the use of data.”
We need to make sure that the nations are sharing information and they’re cooperating with each other, which due to complex relationships, is sometimes difficult. This creates a challenge for customers too.

The second challenge is resource constraint as they have limited budgets and a lack of skilled manpower with customers. When it comes to cybersecurity, the digitalization has happened so fast in our region that it’s getting difficult for businesses to keep pace with the cloud adoption. Therefore, it’s getting challenging for customers to manage all of this with their limited budget.

Thirdly, it’s getting really difficult to always keep upgrading and choosing your network making sure it’s always up to date and protected. The attackers are getting very smart and are doing targeted attacks, so it’s better for companies to adopt cyber resilience, which isn’t just getting yourself protected, but getting ready in case these attacks happen, what is your readiness and how well you are equipped to come back to or to mitigate these threats and make sure that your business suffers minimal damage and you are back up and running to serve your customers and clients.

Cyber resilience is one of the challenges we are seeing, so partners need to educate their customers and every company can develop it with the help of Sophos range of products and services. That’s our goal for partners.

How important is an event like GITEX Global for your company — and what value does it bring for your organisation?

Sophos has been participating at GITEX for more than 14 years, and this has been one of the best leading platforms for us to demonstrate all our product launches and services. It’s a platform where we exchange knowledge and get some information on direct conversations, with not only existing customers, but also potential prospects. We get to learn about what’s the new thought process of the business, what CSOs are thinking about it, what their priorities are for the upcoming years and what the major issues are.

This platform gives us the direct engagement with customers and our partners. We’ve been busy working with all the partners, but this is the time when we talk about not exactly business, but rather logistics discussions with each other about their growth plans and market trends.

From your company’s perspective, what are the key technologies and trends that you’re seeing that will drive your innovation and product roadmap for the next 12 months?

We have recently launched Sophos incident response service for 45 days for any customers, which are actually in active threats or active attacks, and they need help with those tasks. This means rather than going into all the red tape processes, they can directly come to us within a day and we’ll start working to make sure we mitigate and utilize those threats and we provide them 24/7 for 45 days monitoring services to ensure they are now stable and there are no such attacks happening. This is one of the key services we have launched.

Apart from that, we are also working very actively in our network firewall space. ZTNA services and cybersecurity as a service for our customers. We are also working on launching new access points and Wi-Fi six days access points for the market. We are constantly developing our AI based spoofed intel model and driving more automation to reduce the noise level of attacks.

**CONTINUED FROM PAGE 1 Resecurity...**

Identity Protection (IDP) solution will assist countless consumers and companies in the UAE in pursuing this goal. Victims of cybercrime will have the means to safeguard their accounts and personal data through continuous monitoring and proactive early-warning notifications.

**CONTINUED FROM PAGE 1 Sophos...**

From your company’s perspective, what are the biggest challenges businesses are facing and how do you work with partners to solve these?

There are a couple of challenges in the GCC region. One is a geopolitical challenge as we need to make sure that the nations are sharing information and protection. We are trying to educate our partners to move away from coin product selling and go into more of training advisor role for their customers. This means you have to start adding a layer of services to your customers. We’re trying to train them to become a kind of managed service providers, so they engage daily with their customers.

From your company’s perspective, what are the biggest challenges businesses are facing and how do you work with partners to solve these?

There are a couple of challenges in the GCC region. One is a geopolitical challenge as we need to make sure that the nations are sharing information and protection. We are trying to educate our partners to move away from coin product selling and go into more of training advisor role for their customers. This means you have to start adding a layer of services to your customers. We’re trying to train them to become a kind of managed service providers, so they engage daily with their customers.

The availability of this groundbreaking service in the UAE follows the introduction of the second cycle of Dubai’s Cyber Security Strategy by Sheikh Hamdan. This strategy aims to create a society that is safe from cyber threats, and Resecurity’s Identity Protection (IDP) solution will assist countless consumers and companies in the UAE in pursuing this goal. Victims of cybercrime will have the means to safeguard their accounts and personal data through continuous monitoring and proactive early-warning notifications.
Flash forward to the future

All flash for every budget. Simple, secure, and sustainable.

For more information contact: netapp@logicom.net
or visit: https://distribution.logicom.net/netapp/
Mozn and UAE-based Astra Tech Partner To Fortify Fintech Security Via AI-Capabilities

The AI powerhouse forges strategic alliance with the tech pioneer to unleash innovation and security in fintech.

Mozn—by combining our AI-driven compliance solutions with Astra Tech’s unique business model, we’re setting a new industry benchmark for rigorous compliance and financial fraud prevention. The dynamism and growth potential of the UAE market inspires us, and we are uniquely positioned to address its compliance complexities. Together, we’re not just expanding our geographical footprint; we’re strengthening the very fabric of global financial security.”

Abdallah Abu Sheikh, Founder of Astra Tech & CEO of Botim

Mozn and Astra Tech forge strategic alliance to fortify fintech security via AI capabilities.

Mozn, a leader in enterprise-grade mobile app platform, and Astra Tech, a pioneer in UAE-based fintech solutions, have today announced a strategic partnership to fortify the financial sector with AI-powered fintech security solutions.

The collaboration leverages Mozn’s advanced AI capabilities, including advanced data protection, disaster recovery, and security services, combined with Astra Tech’s expertise in fintech management and operations.

**What is the collaboration about?**

Mozn and Astra Tech have formed a strategic partnership to fortify the financial sector with AI-powered fintech security solutions. The collaboration leverages Mozn’s advanced AI capabilities, including advanced data protection, disaster recovery, and security services, combined with Astra Tech’s expertise in fintech management and operations.

**What are the main benefits of the partnership?**

The partnership between Mozn and Astra Tech offers several key benefits, including:

- Enhanced data protection and disaster recovery services
- Advanced security features, such as intrusion detection and prevention
- Customized solutions that can be tailored to specific industry needs
- Improved operational efficiency and compliance

**Who is involved in the partnership?**

Mozn and Astra Tech are the key players in this strategic partnership. Mozn is a leader in enterprise-grade mobile app platform, while Astra Tech is a pioneer in UAE-based fintech solutions.

**What are the key features of Mozn’s AI capabilities?**

Mozn’s AI capabilities include:

- Advanced data protection and disaster recovery services
- Advanced security features, such as intrusion detection and prevention
- Customized solutions that can be tailored to specific industry needs
- Improved operational efficiency and compliance

**What is Astra Tech’s expertise in the fintech sector?**

Astra Tech has established itself as a leader in the UAE fintech sector, offering comprehensive solutions to financial institutions.

**Where is the partnership targeted?**

The partnership is targeted at the financial sector, specifically in the UAE market. The collaboration aims to leverage AI technology to enhance security and compliance, while also offering advanced data protection and disaster recovery services.

**How does the partnership benefit Mozn?**

The partnership benefits Mozn by expanding its market reach into the financial sector, and by leveraging Astra Tech’s expertise in fintech management and operations.

**How does the partnership benefit Astra Tech?**

The partnership benefits Astra Tech by providing access to Mozn’s advanced AI capabilities, which can be leveraged to enhance security and compliance, while also offering advanced data protection and disaster recovery services.

**What is the next step for the partnership?**

The next step for the partnership is to implement the AI-powered fintech security solutions, offering financial institutions a comprehensive suite of services designed to enhance security and compliance, while also offering advanced data protection and disaster recovery services.

**What is the timeline for the partnership?**

The timeline for the partnership is currently not specified, but it is expected to roll out over the next few months.

**Who are the key decision-makers in the partnership?**

The key decision-makers in the partnership are Mozn’s CEO, and Astra Tech’s Founder.

**What is the impact of the partnership on the financial sector?**

The impact of the partnership on the financial sector is expected to be significant, as it will provide financial institutions with advanced AI-powered fintech security solutions, enhancing security and compliance, while also offering advanced data protection and disaster recovery services.

**What is the future vision for the partnership?**

The future vision for the partnership is to expand its reach into other markets, leveraging Mozn’s advanced AI capabilities and Astra Tech’s expertise in fintech management and operations, to offer comprehensive solutions to financial institutions globally.
At GITEX Global 2023, DigiGlass by Redington, a leading technology integrator and innovation powerhouse, is highlighting its revolutionary Security Operations Center, reaffirming its commitment to re-imagining cybersecurity in the digital age. The MESSP brand’s participation at the iconic five-day tech show revolves around three facets – offering AI-embedded advanced capabilities in cybersecurity, preventing disruptions with robust OT security, and leveraging data analytics to safeguard businesses from emerging threats.

AI is pivotal in fortifying cybersecurity, offering unique capabilities to identify, thwart, and counteract evolving cyber threats. Through sophisticated algorithms, AI can scrutinize extensive datasets, pinpointing irregular patterns indicative of potential cyber threats or suspicious activities. Spanning anomaly detection, real-time threat intelligence, predictive analysis, and automated incident response, organizations can significantly strengthen its cybersecurity resilience. Equally vital is the establishment of a resilient OT security strategy, safeguarding industrial control systems and critical infrastructure from cyber threats. At a time when cyber threats are growing in complexity, DigiGlass signifies a revolutionary change in cybersecurity solutions.

DigiGlass’ SOC has expanded over the last few months, in response to escalated threat landscape, and offers continuous monitoring of network traffic. It is a comprehensive cybersecurity framework designed to safeguard organizations against evolving cyber threats and vulnerabilities. DigiGlass’ SOC is a centralized unit embedded with capabilities for monitoring and managing customers’ security hygiene. It comprises cloud-based cybersecurity and OT security offerings with country-specific data sovereignty compliance. Customers can benefit from the completely automated framework and monitor their environments within a single pane of glass.

Dharshana Kosgalage, Head of Technology Solutions Group, Redington Middle East and Africa, said, “DigiGlass by Redington uses threat intelligence and machine learning to proactively identify and mitigate advanced cyber threats. DigiGlass’ SOC has expanded over the last few months, in response to escalated threat landscape, and offers continuous monitoring of network traffic, user behavior, and system activities, providing real-time insights into potential security risks. At GITEX Global, we are hosting thought leadership sessions and showcasing our comprehensive portfolio of solutions to help customers safeguard their digital future.”

Meet the DigiGlass by Redington experts at Stand A1 in Hall 5 to know more on how you can re-imagine your cybersecurity strategies for the digital future.
Juniper Networks expands on AIOps leadership with new UAE Local Cloud Instance

Juniper Networks, a leader in secure, AI-driven networks, recently announced that its wireless access, wired access, NAC, indoor location and SD-WAN solutions, all driven by Mist AI, will have a local cloud instance in the UAE. Juniper customers and partners in the region will receive the benefits of a cloud native architecture, which includes microservices agility, resiliency and elastic scale, as well as local hosting and storage. In the Middle East, it is becoming increasingly important to validate where data is stored due to data privacy and cybersecurity concerns. The launch of the Juniper UAE Cloud instance helps to align with security standards, enabling Juniper to deliver more secure, resilient and automated AI-driven cloud services in support of digital transformation initiatives while their data is stored on a locally hosted cloud. The Juniper Mist solutions deliver unsurpassed automation, insight and assurance for simplified operator experiences and exceptional user experiences. The entire Juniper campus and branch portfolio is managed via a common Mist cloud and AI engine for assured client-to-cloud experiences across the wired, wireless and WAN domains. Proactive actions and self-driving network operations avoid problems before they arise, eliminating as many as 90 percent of in-bound trouble tickets.

Juniper has also been named as a Leader in the 2022 Gartner® Magic Quadrant™ for Enterprise Wrenched and Wireless LAN Infrastructure for the third consecutive year, with Juniper being placed highest in execution and vision. The company is recognised as the only Visionary in the 2023 Gartner® Magic Quadrant™ for SD-WAN. Many UAE organisations integrate cloud-driven AI services into their broader IT strategies, making cloud services essential for the future. Juniper has seen substantial traction for our AI-driven campus and branch portfolio with top enterprises choosing the company’s best-in-class solutions, operated via the cloud. To further boost this momentum, Juniper will offer a strong cloud instance in the UAE, promoting digital transformation, spurring innovation and reducing operational costs throughout the UAE.

“Cloud adoption is snowballing in the Middle East, driven by widespread efforts by organisations to modernise their infrastructure and applications. There is also a significant shift in the regulatory environment, which is pushing companies towards secure and compliant cloud solutions. As a result, most enterprises in the region are increasingly preferring locally hosted cloud solutions.” – Mark George, Senior Research Manager – Software & Cloud, IDC Middle East, Turkey & Africa

Avaya unveils cutting-edge solutions for enhanced customer experiences

Veronica Martin spoke to Ahmad Dorra, Customer Engagement Solutions Sales Leader MEA & Turkey at Avaya to discuss their new products and solutions and GITEX Global, the key technologies and trends driving innovations and how important GITEX Global is for Avaya.

Can you tell our readers what new products and solutions you are demonstrating and launching here this week at GITEX Global?

We, at Avaya, are a leader in customer experience solutions and have been helping a lot of brands and government entities guide them towards reaching their desired customer experience. As we know each organisation has a unique position in their customer experience journey, this insight leads us as a buyer to deliver a unique approach to our customers.

This year we are looking at the new branding and customer experience integrating AI in all verticals. This means we are implementing generative AI beyond just the personas that we used to demonstrate before and taking it across all personas within the organisation in order to empower all employees at all levels.

From your company’s perspective, what are the key technologies and trends that you’re seeing that will drive your innovation and product roadmap for the next 12 months? Generative AI is the evolution of AI and the key trend today’s market. We are seeing all customers want to adopt to the digital transformation and also a big hype on analytics, as they really want to leverage their analytics to understand how their business is going and what people are talking about their brands. We are focusing to deliver this style of innovation to our customers, but, at the same time, we need to make sure that we’ll deliver without disrupting their current operation. That’s what we call it, innovation without disruption.

How important is an event like GITEX Global for your company — and what value does it bring for your organisation? GITEX has become a huge worldwide and a great opportunity for us to demonstrate our power, what we are doing to become more innovative and what we can deliver to our customers. Besides, we will be showing our customers how we can integrate our technology without disrupting their journey. They can choose their journey at their own pace, and we are here to support them to deliver it in the most effective way.
Catalyst of change

Anita Joseph caught up with Ranjith Kasapooraya, MD, Cloud Box Technologies, to find out how the company is playing a pivotal role in safeguarding businesses against evolving cyber threats and ensuring seamless digital transformation.

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

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

At CBT, we focus on designing a seamless digital transformation, Cloud Box Technologies (CBT) steps in as an expert consultant, guiding businesses through a step-by-step progression in this transformative process. The key is that each customer’s journey is unique. CBT tailors its solutions to the needs of each client, capitalising on digital technologies to elevate businesses to the next level. Since every customer has a unique profile, it makes it impossible to standardise digital transformation technology or processes across all companies. Therefore, it is important for us to base our approach on understanding each customer’s experience and focus on the key areas where digital transformation can make an impact. At CBT, we analyse the various digital transformation solutions that can elevate businesses to the next level, acting as a catalyst for this transformation. For instance, the requirements for a hospitality organisation might differ from those of a retail business or the banking sector. Precisely comprehending each customer’s needs is a fundamental step. Investing in data and analytics is a significant undertaking, albeit necessary. However, while the market offers numerous reporting and data analytics tools, the question of investment readiness arises. As a System Integrator, we firmly believe in the necessity of these tools to drive transformation. Guiding customers towards the right product and tool is a crucial step, as effectively consolidating and deriving valuable insights from data is a key service we provide. Stepping into the realm of technology, we leverage our expertise to guide customers through the adoption of new technologies. Our approach varies based on the specific industry, be it healthcare, banking, or others. While our uniqueness lies in our ability to understand challenges, success hinges on effectively communicating and providing accurate information to customers. Our role is to understand industries, recommend the most suitable technologies for business profitability and cost reduction, and guide customers seamlessly through the whole process. In short, as the momentum behind digital transformation gains traction, CBT acts as an advocate for customers, providing expert guidance that ensures a smooth and purposeful digital transformation journey. Instead of offering standardised solutions, CBT pinpoint’s core areas where effective transformation is required based on each customer’s unique experience and objectives.

For digital transformation to be seamless, there needs to be the right set of skills. Do you think that it only requires a skilled workforce out there today to meet the demand for digital technology implementation? How does Cloud Box Technologies address the scarcity of skilled professionals?

An important aspect of skilled professionals is a pressing issue in today’s market. Convincing CEOs and investors of the importance of technology adoption can be challenging, particularly with the understanding of its implications often varying widely between skilled executives and the general workforce. Bridging this gap requires a bottom-up approach, where employees across all levels better comprehend the significance of digital transformation. CBT recognises this necessity and employs a specialised team of skilled engineers who possess the expertise to understand customer needs and effectively facilitate the technology transformation. We ensure that the right skill sets are in place to guide clients through successful digital transformation.

We step in as a specialised technology partner, tailoring ourselves from other resellers by being a Value-Added Service Provider. Our focus is not broad; rather, it is specific, verticals and, at present, our strength lies in the healthcare sector, along with hospitality and banking. Our team excels in identifying gaps within individual verticals, enabling us to pinpoint the necessary skill sets to address specific needs. Our team is primarily made up of technically skilled engineers who have a deep understanding of customer requirements and provide the right guidance. To ensure success is underscored by the simultaneous management of nearly a dozen products, ensuring that our experts are strategically positioned to guide customers through a successful digital transformation journey.

This track record of accomplishment has led to an increasing trust in our capabilities year after year.

Can you elaborate on the significance of Security Operations Centers (SOCs) in today’s landscape and how CBT contributes to successfully addressing advanced cyber threats?

Digital transformation is an isolated activity. It is not just enough to merely focus on extensive technological changes, safeguarding these investments also becomes paramount. Security Operations Centers (SOCs) play a crucial role in this context. As the understanding of its implications often varies widely between skilled executives and the general workforce, bridging this gap requires a bottom-up approach, where employees across all levels better comprehend the significance of digital transformation. CBT recognises this necessity and employs a specialised team of skilled engineers who possess the expertise to understand customer needs and effectively facilitate the technology transformation. We ensure that the right skill sets are in place to guide clients through successful digital transformation.

Our SOC service can effectively consolidate and derive valuable intelligence from new technology messages. At CBT, we ensure that potential threats are identified and mitigated, setting us apart in the market.

Our SOC service can effectively consolidate and derive valuable intelligence from new technology messages. At CBT, we ensure that potential threats are identified and mitigated, setting us apart in the market. This holistic approach safeguards against data loss and ensures rapid recovery in the event of an attack, setting us apart in the market. Our SOC service can effectively consolidate and derive valuable intelligence from new technology messages. Our SOC service can effectively consolidate and derive valuable intelligence from new technology messages.

So, what CBT’s go-to market strategy going to be, for the GCC market in particular?

Our strategy revolves around teamwork, collaboration, and differentiation. Rather than serving as a mere intermediary, CBT positions itself as a digital transformation enabler. By bridging the gap between vendors and customers, CBT ensures that technology messages are effectively translated and implemented. This unique approach has earned CBT a reputation as a premium cluster System Integrator, with a focus on skilled engineering, deep understanding of the threat landscape, and the capacity to anticipate new attack vectors before they even arise.

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

CBT's strategy revolves around teamwork, collaboration, and differentiation. Rather than serving as a mere intermediary, CBT positions itself as a digital transformation enabler. By bridging the gap between vendors and customers, CBT ensures that technology messages are effectively translated and implemented. This unique approach has earned CBT a reputation as a premium cluster System Integrator, with a focus on skilled engineering, deep understanding of the threat landscape, and the capacity to anticipate new attack vectors before they even arise.

Our SOC service can effectively consolidate and derive valuable intelligence from new technology messages. At CBT, we ensure that potential threats are identified and mitigated, setting us apart in the market.

Can you provide an overview of the comprehensive solutions portfolio offered by CBT, including the key services and how they contribute to the overall digital transformation strategy of businesses?

The CBT SOC will support customers with the following:

- Continuous Protection - 24/7 uninterrupted monitoring of systems to detect potential threats.
- Security Intelligence - Using the latest technologies, we help our clients identify and mitigate cyber threats in real-time.
- Quick and Effective Risk Management - An innovative approach to advanced technology, with our expertise helping clients detect threats and respond to mitigate risks quickly.
- Threat prevention - Effective monitoring of the threat landscape to provide an awareness view of the network and anticipate new threat vectors before they even emerge.
- Proactive incident response strategies - We offer a thorough and comprehensive response to threats in real-time, reducing risk of data breaches or cyber-attacks and help identify any potential weaknesses that can be exploited.
- Cost Savings - We utilise the latest technologies to ensure that our services meet the requirements of our clients. Our SOC service ensures that technology messages are effectively translated and implemented. This unique approach has earned CBT a reputation as a premium cluster System Integrator, with a focus on skilled engineering, deep understanding of the threat landscape, and the capacity to anticipate new attack vectors before they even arise.
Kaspersky and SADAFCO elevate cyber literacy in a critical infrastructure sector

Kaspersky and Saudia Dairy and Food Stuff Company have collaborated to share practices and improve cybersecurity awareness within the Middle East’s critical infrastructure sector.

The food industry is part of the critical infrastructure sector and protecting it against evolving cyberattacks from different threat actors is a national priority in Saudi Arabia*

Kaspersky and Saudia Dairy and Food Stuff Company

*To understand more about the ICS threat landscape, meet the Kaspersky experts at Stand H25-A31, Hall 25 at GITEX Global 2023, or read more here.

To keep your OT computers protected from various threats, Kaspersky experts recommend:

- Conducting regular security assessments of OT systems to identify and eliminate possible cyber security issues.
- Establishing continuous vulnerability management processes.
- Improving the environmental, social, and corporate governance (ESG) metrics.
- Review and evaluate cybersecurity and data privacy governance processes.
- Track your company’s KPIs against committed ESG metrics.
- Maintain transparency on cybersecurity measures across all levels of the workforce via regular corporate communications.

“...When it comes to ICS, all world regions have their specifics. The Middle East is a major global energy hub, with numerous critical infrastructure facilities, including oil and gas refineries. Protecting these facilities from cyber threats is of paramount importance to ensure a stable energy supply worldwide. It should also be noted that many Middle Eastern countries are undergoing rapid industrialisation and modernisation, often involving the deployment of new ICS technologies. These systems may not have robust cyber security management processes, making them potential targets,” comments Evgeny Goncharov, Head of Kaspersky ICS CERT.

“By understanding the risks related to ICS, organisations can make informed decisions, allocate resources wisely, and efficiently fortify their defenses. In doing so, they not only protect their bottom line but also contribute to a safer and more secure digital ecosystem for all.”

Mission critical applications heavily leverage critical infrastructure sector assets and can suffer major financial losses or even complete service disruptions due to the interruption of the production process.

As digital transformation worldwide, it should be evident that ensuring a stable energy supply and efficient and reliable commerce is crucial for preventing a major incident that might cost millions due to the interruption of the production process.

In the current world, companies such as Kaspersky Endpoint Detection and Response for timely detection of sophisticated threats, investigation, and effective remediation of incidents.

Improving the response plan and advanced malicious techniques by building and strengthening your teams’ incident prevention, detection, and response skills.

Dedicated OT security training for IT security teams and OT personnel is one of the key measures helping to achieve this.

To equip your organisation with the right knowledge and tools, SADAFCO recommends:

- With one wrong tick potentially having major security consequences, educating and training the workforce is a priority; it is the first line of defense against malicious attacks.
- Implement robust Environmental, Social, and Corporate Governance (ESG) practices that ensure strategic and operational alignment across all parts of the business.
- Review and evaluate cybersecurity and data privacy governance processes.
- Track your company’s KPIs against committed ESG metrics.
- Maintain transparency on cybersecurity measures across all levels of the workforce via regular corporate communications.

Mission critical applications heavily leverage critical infrastructure sector assets and can suffer major financial losses or even complete service disruptions due to the interruption of the production process.

As digital transformation worldwide, it should be evident that ensuring a stable energy supply and efficient and reliable commerce is crucial for preventing a major incident that might cost millions due to the interruption of the production process.

In the current world, companies such as Kaspersky Endpoint Detection and Response for timely detection of sophisticated threats, investigation, and effective remediation of incidents.

Improving the response plan and advanced malicious techniques by building and strengthening your teams’ incident prevention, detection, and response skills.

Dedicated OT security training for IT security teams and OT personnel is one of the key measures helping to achieve this.

To equip your organisation with the right knowledge and tools, SADAFCO recommends:

- With one wrong tick potentially having major security consequences, educating and training the workforce is a priority; it is the first line of defense against malicious attacks.
- Implement robust Environmental, Social, and Corporate Governance (ESG) practices that ensure strategic and operational alignment across all parts of the business.
- Review and evaluate cybersecurity and data privacy governance processes.
- Track your company’s KPIs against committed ESG metrics.
- Maintain transparency on cybersecurity measures across all levels of the workforce via regular corporate communications.
Are you confident your infrastructure can prevent a non-tolerable event?

Too many companies with SOC2/ISO27001/PCI DSS certifications have been hacked.

We treat threats differently to ensure no intolerable damage occurs. Ever.

global.ptsecurity.com
What is coming ‘Next’

CNEF Editor Mark Parker attended ‘Next’ 23 in San Francisco, as Google Cloud ushered in a new cloud era, one that will be driven by advancements made in generative AI.

Customer momentum:
Organizations across industries and around the world are placing demands on Google Cloud to digitally transform, and this year they have shared stories from Culture Amp, Deutsche Börse, eDreams ODIGEO, Government of Singapore, HSBC, IHP, IFPG Medbrands, John Lewis Partnership, The Knot Worldwide, Macquarie Bank, Mayo Clinic, Priceline, Shopify, U.S. Steel, and many more. In addition to this, Google Cloud also announced the expanded relationships with The Estée Lauder Companies, GE Appliances, General Motors, HCA Healthcare, and more.

Innovative gen AI startups, like Repli, Typetac, Jasper, and more, are eagerly choosing to build on Google Cloud. In fact, more than half of all funded gen AI startups—including companies like Contextual, CoRover, Elementary Cognition, Fiddler, Sheetailor, and Google Cloud customers. This includes 70% of all gen AI unicorns, like AI2, Anthropic, Cohere, Runway, and others.

New infrastructure and tools to help customers:

- The advanced capabilities and broad applications that make gen AI so revolutionary demand the most sophisticated and capable infrastructure. Google Cloud is enabling key infrastructure advancements to help our customers:
  - Cloud TPUs: This is Google Cloud’s most cost-efficient, versatile, and scalable AI platform—Vertex AI—that makes adapter tuning generally available, while introducing a new method for images, called Style Tuning, so enterprises can create images aligned to brand guidelines with a small amount of reference images.
  - New models: Google Cloud is announcing availability of Llama 2 and Codex, as well as an open-source model, as well as pre-announcing Claude 2 from Anthropic. Google Cloud will be the only cloud provider offering both adapter tuning and RLHF for Llama 2.
  - Data Cloud: Developers can access, build, and manage extensions that deliver real-time integrations, incorporate company data, and take action on the user’s behalf.
  - Digital Watermarking: Our models now have access to more than 3 billion users and more than 10 million paying customers who rely on it every day to get things done.

With the introduction of Duet AI at I/O last year, Workspace evolved, introducing a number of features to help users make more productive, like helping write and refine content in Google Docs and Google Sheets, create original images in Google Slides, turn ideas into action, and data into insights with Google Sheets, foster more meaningful connections in Google Docs and Google Chat, and more.

New enhancements announced today include:
- Duet AI at Work: Duet AI will take notes during video calls, send meeting summaries, and even automatically translate captions in 18 languages. Duet AI at Work is available today.
- Google Cloud Office: Google Cloud is launching a comprehensive breakdown on the new parallelisms forged, new infrastructure and tools rolled out and the expansion of the Vertex and Duet AI by Google Cloud.

We want to help every person use AI, and we want to bring together the whole AI ecosystem so they can succeed in adopting AI.

“I believe that we are only really starting to scratch the surface since when we made Vertex AI available. Our objective is to equip our customers with access to the right tools for them to create and innovate. In terms of Duet AI, we already have 1.5 million users, and today, we are delighted to announce the general availability of Duet AI at Google Workspace,” said Pichai.

Pichai also spoke of his address by declaring that the company will continue to be bold and provide scalable, and said they are imparting on a ‘golden age’ of innovation.

Thomas Kurian kicked off his keynote by saying that the shift to AI will represent one of the most profound changes in our lives. He reiterated Google’s mission, which is to help every person to be able to use AI. “Our generative AI products are delivering real results in every single discipline. We want to help every person use AI, and we want to bring together the whole AI ecosystem so they can succeed in adapting AI,” said Kurian.

Kurian outlined how customers were increasingly drawn to their work-class infrastructure, revealing that Yahoo is migrating 500 million mailboxes and 50PB of data to Google Cloud as part of their efforts to improve their e-commerce experience, whilst Mahindra Riss has utilised the capabilities of Google Cloud to help them sell over 100,000 SUVs.

Kurian highlighted the impact some of their new products have in terms of delivering productivity and operational gains for their customers.

“Today, we are launching a new product called GKE Enterprise, which has been designed to enable multi-cluster horizontal scaling. Customers have already seen an increase of 45% in productivity gains, whilst reducing software deployment times by over 70%,” said Kurian.

In addition to this, Kurian spoke of their excitement at their partnership with NVIDIA.

“We’re also announcing the availability of our A3 VMs, based on NVIDIA’s A3-IoT. With A3-IoT, GKE Enterprise will offer customers:
- PaLM 2, Imagen and Codex: This includes updating PaLM 2 to 32k context windows so enterprises can easily process longer form documents like research papers and books.
- Tools for tuning: For PaLM 2 and Codex, Google Cloud is making adapter tuning generally available, and introducing a new method for images, called Style Tuning, so enterprises can create images aligned to brand guidelines with a small amount of reference images.
- New models: Google Cloud is announcing availability of Llama 2 and Codex, as well as an open-source model, as well as pre-announcing Claude 2 from Anthropic. Google Cloud will be the only cloud provider offering both adapter tuning and RLHF for Llama 2.
- Data Cloud: Developers can access, build, and manage extensions that deliver real-time integrations, incorporate company data, and take action on the user’s behalf.
- Digital Watermarking: Our models now have access to more than 3 billion users and more than 10 million paying customers who rely on it every day to get things done.”
Smart security for every home.

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

Ring... smart security for every home.

ring
an amazon company

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

To learn more, visit us at GITEX Global 2023 Stand H20-B05
Tencent Cloud Empowers MEA Enterprises with New SuperApp-as-a-Service, AI and Media Capabilities

Tencent Cloud’s second year of participation in the significant tech event underscores company’s commitment to growing its cloud business in the MEA market. The showcase also features the digital platform upgrade for Abu Dhabi’s government services.

Tencent Cloud, the cloud business of global technology company Tencent, showcased its digital platform upgrade for Abu Dhabi’s government services. Tencent Cloud is looking to strategically grow its business in the Middle East and Africa (MEA) market, demonstrating its unique value in solving security and sustainability challenges.

During the event, Tencent Cloud highlighted its SuperApp-as-a-Service, along with its latest innovations in cloud security solutions. The Tencent Cloud AI and media platform family, that will be taken on tour by regional leaders. Leveraging the track record in supporting WeChat’s ecosystem with over 1.1 billion monthly active Mini Program users, Tencent Cloud’s SuperApp-as-a-Service features the Tencent Cloud Mini Program Platform (TPMP) that transforms web and mobile apps into one lightweight service for aggregation, open to any cloud infrastructure with local cloud services support.

This platform offers a robust digital infrastructure which is fundamental for enterprises and public service transformation.

The showcase, held on 13 October 2023, under the Department of Government Services, is a collaborative platform for the Emirate of Abu Dhabi, placing a focus on the digital transformation of its essential public services. The event will also showcase products including customer service, a vast variety of fields, for digital avatars across the Middle Eastern market, as gaming solutions, for digital transformation.

Tencent Cloud Smart Video Analysis Platform, also will showcase their advanced capabilities to help media organizations, enterprises, and content creators in areas such as video content gathering, editing, moderation, and smart video analytics.

Dan Hu, President of Tencent Cloud International for the Middle East and Africa, said, “Our ecosystem building experience in the consumer information infrastructure, with AI capabilities accumulated, including hosting apps and offering internet infrastructure, for a billion users. Tencent Cloud is well positioned to work with local partners in the MEA region to support the local public service transformation, enabling enterprises and international businesses to leverage Tencent technologies to access the Chinese market, in addition to undertaking their own digital transformations in local markets using Tencent products and services.”

Patric Ramseyer, Vice President, EMEA at LinkShadow discusses the importance of intelligent NDR – and how his company is steering CISOs away from the traditional siloed approach to cybersecurity.

Patric Ramseyer is an Irish Swiss national who has enjoyed a stellar career in the security industry. He has spent most of his professional life in Switzerland and has moved to the UAE in 2021, where he was appointed as the Managing Director of a well-knowncéan operation. In April of this year, he joined LinkShadow, where he has been tasked with the responsibility of driving their growth across the MEA region.

In a candid discussion with CNME, Patric Ramseyer was transparent on the issues facing CISOs in the current cyber climate, and how the solutions within their product portfolio are equipped with the tools they need to both protect their assets and improve their security posture. He kicked off the conversation by highlighting the need for large enterprise to adopt a cloud-based approach to security.

“One of the major challenges that stakeholders and CISOs are encountering is with the fact that they have what would be described as a siloed approach. Essentially, that means they are building up their security operations centered around various teams for various products. For example, take a CISO with a team of 50 people working for them, he has a firewall team, end point detection and response team, but they are all working in separate little silos, and ultimately what leads to is a lot of noise. When we say noise in security operations what we talk about are false positives, which is basically security professionals investigating or responding to events that aren’t important, and that leads to ‘alert fatigue’,” said Ramseyer.

As Ramseyer pointed out, the lack of talent and skills on a global scale has fostered an environment in which staffing shortages is the norm.

“If you work in an air traffic control tower you work like that, so you stop and take a 35-minute break because of the sheer pressure. However, security operations centres don’t work like that because they can’t afford to have a break. If for him, he has a firewall team, end point detection and response team, but they are all working in separate little silos, and ultimately what leads to is a lot of noise. When we say noise in security operations what we talk about are false positives, which is basically security professionals investigating or responding to events that aren’t important, and that leads to ‘alert fatigue’,” said Ramseyer.

Patric Ramseyer

Patric Ramseyer is a cybersecurity expert who has been involved in the industry for over 20 years. He has held various roles in both private and public sectors, including as a Senior Advisor at the United Nations and as a Lecturer at the University of Cambridge. He is currently the Chief Security Officer at LinkShadow, a leading cloud security provider.

Patric Ramseyer

Patric Ramseyer is a cybersecurity expert who has been involved in the industry for over 20 years. He has held various roles in both private and public sectors, including as a Senior Advisor at the United Nations and as a Lecturer at the University of Cambridge. He is currently the Chief Security Officer at LinkShadow, a leading cloud security provider.

Patric Ramseyer

Patric Ramseyer is a cybersecurity expert who has been involved in the industry for over 20 years. He has held various roles in both private and public sectors, including as a Senior Advisor at the United Nations and as a Lecturer at the University of Cambridge. He is currently the Chief Security Officer at LinkShadow, a leading cloud security provider.

Patric Ramseyer

Patric Ramseyer is a cybersecurity expert who has been involved in the industry for over 20 years. He has held various roles in both private and public sectors, including as a Senior Advisor at the United Nations and as a Lecturer at the University of Cambridge. He is currently the Chief Security Officer at LinkShadow, a leading cloud security provider.

Patric Ramseyer

Patric Ramseyer is a cybersecurity expert who has been involved in the industry for over 20 years. He has held various roles in both private and public sectors, including as a Senior Advisor at the United Nations and as a Lecturer at the University of Cambridge. He is currently the Chief Security Officer at LinkShadow, a leading cloud security provider.

Patric Ramseyer

Patric Ramseyer is a cybersecurity expert who has been involved in the industry for over 20 years. He has held various roles in both private and public sectors, including as a Senior Advisor at the United Nations and as a Lecturer at the University of Cambridge. He is currently the Chief Security Officer at LinkShadow, a leading cloud security provider.

Patric Ramseyer

Patric Ramseyer is a cybersecurity expert who has been involved in the industry for over 20 years. He has held various roles in both private and public sectors, including as a Senior Advisor at the United Nations and as a Lecturer at the University of Cambridge. He is currently the Chief Security Officer at LinkShadow, a leading cloud security provider.

Patric Ramseyer

Patric Ramseyer is a cybersecurity expert who has been involved in the industry for over 20 years. He has held various roles in both private and public sectors, including as a Senior Advisor at the United Nations and as a Lecturer at the University of Cambridge. He is currently the Chief Security Officer at LinkShadow, a leading cloud security provider.

Patric Ramseyer

Patric Ramseyer is a cybersecurity expert who has been involved in the industry for over 20 years. He has held various roles in both private and public sectors, including as a Senior Advisor at the United Nations and as a Lecturer at the University of Cambridge. He is currently the Chief Security Officer at LinkShadow, a leading cloud security provider.
we’re taking to your EDR, IDDs, and firewall teams, and we’re correlating and aggregating all this information, and that’s where our AI and Machine Learning comes in, because you can’t do that manually, the only way to do it is by using adaptive AI. The other element is being able to correlate the automation of all the responses, and that’s all done using our AI engine,” said Ramseyer. However, according to Ramseyer the biggest question that underpins all of this above is how do businesses save money?

“A CISO will say to you that I need you to hand me a proposal that I can give to my CFO that demonstrates that if we purchase this product then we’re going to save money. You can show the cost savings very, very quickly, and the primary reason for that is the fact we have one user interface. For example, if I take this siloed approach, then I’ll have 10 different types of interfaces, and 10 different panes of glass. Every vendor will tell you that they have a single pane of glass, but it’s 10 altogether, it’s not a single pane of glass. You have to take all those 10 interfaces and funnel them into one. By doing that you have one platform that shows you where your threats are, how to respond to the threats – and ideally it will tell you where you are wasting money. In addition to this, if you want to investigate further, or if you need a specialist for forensics then you can go into your firewall logs,” said Ramseyer.

Ramseyer also highlighted the issue of “vendor lock-in” that many CISOs and IT directors face. “A lot of CISOs and IT directors will talk to you about vendor lock-in – which essentially means they are rather reliant on one particular vendor. CISOs don’t like that because it takes the decision out of their hands, and maybe one vendor has a better endpoint detection and response than the other, but because they are locked in they can’t use it. They want autonomy and choice. The big advantage we have is that the fact that we integrate with any vendor; it doesn’t matter if your Microsoft, Sophos, or Kaspersky, we integrate with all of them via what is called bi-directional API. We’re not only receiving information from them, we’re also sending them activities in terms of response, so it’s a two-way communication between each of those systems, and we have already gone beyond 90 percent done with all the major vendors, and they’re coming up with that the threats are, so you can say what is going on in each one from the one pane of glass,” said Ramseyer.

LinkShadow has drawn widespread acclaim for their intelligent NDR solution. “A CISO will say to you that I need that one, or do I really need a very expensive one? You could have a DLP system that cost you $30,000, and you can have a DLP system that can cost you $1m, but you might only need a $30,000 one if your DLP is not a major concern, but you need to be able to determine that, and again that’s where we come in. Ultimately, our intelligent NDR empowers CISOs to make the decisions based on the criteria that’s important to them, and the No.1 criteria that’s important to any CISO is money because security is a blackhole when it comes to money,” said Ramseyer.

Another key component within LinkShadow’s intelligent NDR offering is their block count ratio. “We have what we call a block count ratio, and that is that essentially means how many blocks did my security tool do? How many times did it block a blacklisted IP address, how many times did this end-point detection and response cut out malicious files. We can see by assessing each tool how effective they are. We can then give the CISO a lovely report where he sees these intrusion detection systems have only accounted for 8% of their total blocks for a year, which is less than 3%, so does he really need that one, or do he really need a very expensive one? You could have a DLP system that cost you $30,000, and you can have a DLP system that can cost you $1m, but you might only need a $30,000 one if your DLP is not a major concern, but you need to be able to determine that, and again that’s where we come in. Ultimately, our intelligent NDR empowers CISOs to make the decisions based on the criteria that’s important to them, and the No.1 criteria that’s important to any CISO is money because security is a blackhole when it comes to money. Another key component within LinkShadow’s intelligent NDR offering is their block count ratio. “We have what we call a block count ratio, and that is that essentially means how many blocks did my security tool do? How many times did it block a blacklisted IP address, how many times did this end-point detection and response cut out malicious files. We can see by assessing each tool how effective they are. We can then give the CISO a lovely report where he sees these intrusion detection systems have only accounted for 8% of their total blocks for a year, which is less than 3%, so does he really need that one, or do he really need a very expensive one? You could have a DLP system that cost you $30,000, and you can have a DLP system that can cost you $1m, but you might only need a $30,000 one if your DLP is not a major concern, but you need to be able to determine that, and again that’s where we come in. Ultimately, our intelligent NDR empowers CISOs to make the decisions based on the criteria that’s important to them, and the No.1 criteria that’s important to any CISO is money because security is a blackhole when it comes to money. Another key component within LinkShadow’s intelligent NDR offering is their block count ratio. “We have what we call a block count ratio, and that is that essentially means how many blocks did my security tool do? How many times did it block a blacklisted IP address, how many times did this end-point detection and response cut out malicious files. We can see by assessing each tool how effective they are. We can then give the CISO a lovely report where he sees these intrusion detection systems have only accounted for 8% of their total blocks for a year, which is less than 3%, so does he really need that one, or do he really need a very expensive one? You could have a DLP system that cost you $30,000, and you can have a DLP system that can cost you $1m, but you might only need a $30,000 one if your DLP is not a major concern, but you need to be able to determine that, and again that’s where we come in. Ultimately, our intelligent NDR empowers CISOs to make the decisions based on the criteria that’s important to them, and the No.1 criteria that’s important to any CISO is money because security is a blackhole when it comes to money.
STANDS TO WATCH

STARLINK
Stand: H3

Spark Your Growth
ACCELERATING UNICORNS WITH SIA
STARTUPS • ISVs • ALLIANCES

You Can
- Identify Market Gaps
- Ideate and Innovate on Cloud
- Create Disruptive Solutions

We Can
- Provide Dedicated Focus
- Expedite Time to Market
- Aid in Adoption & Innovation

Together We Will
- Build Competency
- Define GTM Strategy
- Align Commercial Strategy
- Drive Marketing Strategy

Talk to Us & Skyrocket Your Unicorn Journey

Visit us at Expand North Star (15-18 Oct) – Hall 7
GO BEYOND LIMITS
WIN BIG
with StorIT & Dell Technologies

SCAN TO SIGN UP

**Valid for Dell Channel Resellers in UAE region only

WIN HARLEY DAVIDSON BIKE
WIN PORSCHE SPORTS CAR
WIN GOLD COINS

StorIT Distribution fzc
Anantara Downtown Business Tower, Business Bay & Jafza 15, Jebel Ali Freezone, Dubai, United Arab Emirates
P.O.Box 17417 | Tel: +971.4.8819890 | Email: info@storit.ae | www.storit.ae
GITEX GLOBAL 2023

Accelerate Intelligence

16 - 20 October
Visit us at Hall 22
#HWGITEX23
Deliver Exceptional Digital Experience with Unified Observability and Acceleration Solutions

Don’t Miss Riverbed at GITEX Global 2023!

Visit Riverbed Technology to explore two industry-leading portfolios that drive enterprise performance and exceptional digital experiences. With Alluvio™’s Unified Observability, transform data into actionable insights to deliver seamless, secure digital experiences for customers and employees. With Riverbed Acceleration, provide fast, agile, secure acceleration of any app, over any network, to users everywhere. Learn more at riverbed.com.

Concourse 2, Booth CC2-18
Dubai World Trade Center
16th – 20th October 2023

@2023 Riverbed Technology L.L.C. All rights reserved.
STANDS TO WATCH

VEEAM

Stand: H7-D20
Secure Your **Digital Future**


Secure Your Enterprise IT Footprint
For A Safer Digital Journey

www.raqmiyat.com
UAE | KSA | INDIA
DOES YOUR DATA PROTECTION LEAVE GAPS?

Question it.

See what makes Commvault the only unified data protection that covers all your data, wherever it lives. Data protection vendors have been throwing around a lot of big claims and buzzwords that could put your data at risk. It’s time to question it all.

COMMVAULT

Learn more at commvault.com/questionit.