WWW.TAHAWULTECH.COM

ADVISOR

**MIDDLE EAST** 

# THE ADDER SHIP AND ATA TELLS SAME HOW HE FELT THREATENED AFTER

FAYEZ IBBINI, CEO OF ALPHA DATA, TELLS SAME HOW HE FELT THREATENED AFTER HIS COMPANY EXPERIENCED A RANSOMWARE ATTACK – AND OFFERS HIS ADVICE ON THE STEPS BUSINESSES NEED TO ADOPT TO MITIGATE THE DAMAGE OF A RANSOMWARE ATTACK.

🔅 tahawultech.com





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

Cybersecurity, everywhere you need it

### www.fortinet.com



Copyright ©2023 Fortinet, Inc. All Rights Reserved.

## CONTENTS

### 





# 2 LEADERSHIP DURING CRISIS



6 News from the world of cybersecurity and beyond

**10** Johan Paulsson, CTO at Axis Communications, predicts the technology trends driving the security sector in 2024 22 Ned Baltagi, Managing Director – Middle East, Turkey, and Africa at SANS Institute, on cybersecurity in the region and how SANS is committed to equipping professionals with the required skills.

**30** Genetec 2024 State of Physical Security Report

# **Solar Powered Camera**

### No network cable required

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

### **Easy installation**

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

### Can withstand bad weather

Prone to extreme weather such as strong wind and rainstorms.



2MP @ 30 fps





**4**G





Scan to Learn More

HIKVISIONMENA in HIKVISION-MENA

O HIKVISIONMENA HIKVISIONMENA





### EDITOR'S NOTE



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

> Anita Joseph Editor

#### **EVENTS**



### **SAFEGUARDING THE HOLIDAYS**

**STAY AHEAD OF** 

ATTACK TRENDS

s we embrace the festive season, our reliance on online platforms for holiday shopping has never been more pronounced. With the convenience of digital transactions, however, comes an inherent risk that demands our attention. In this edition, we bring you crucial insights into fortifying your online shopping experience and staying one step ahead of cyber threats.

As the holiday season unfolds, the allure of irresistible deals can sometimes overshadow the importance of

securing our digital transactions. From utilising secure payment

methods to recognising phishing attempts, we equip you with the knowledge to shop with confidence in the digital marketplace.

In the fast-evolving landscape of cyber threats, it's imperative to stay informed about the latest trends and explore the emerging tactics employed by cybercriminals, ranging from sophisticated ransomware attacks to the manipulation of artificial intelligence for malicious purposes. Understanding these trends is the first line of defense in safeguarding your digital presence. Ransomware, in particular, has seen a surge in both frequency and sophistication. Our in-depth analysis sheds light on the evolving strategies employed by ransomware operators and provides actionable insights to fortify your organisation's cybersecurity posture.

Moreover, as we enter the era of smart homes and interconnected devices, the "Internet of Things (IoT) Security Outlook" explores the potential vulnerabilities

> and best practices for securing your smart home ecosystem. From connected thermostats

to smart doorbells, we unravel the security implications of our increasingly interconnected lives.

In the spirit of a safe and secure holiday season, let this edition be your guide to navigating the digital landscape with confidence. As the year comes to a close, may your online transactions be secure, your personal data protected, and your holidays filled with joy and peace of mind.

Wishing you a cyber-safe and joyful holiday season, Happy Reading!

Published by

Dominic De Sousa (1959-2015)

FOUNDER, CPI

ADVERTISING Group Publishing Director Kausar Syed kausar.syed@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.joseph@cpimediagroup.com PRODUCTION AND DESIGN Designer Prajith Payyapilly prajith.payyapilly@cpimediagroup.com DIGITAL SERVICES Web Developer Adarsh Snehajan webmaster@cpimediagroup.com Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai, UAE

Tel: +971 4 5682993

© Copyright 2023 CPI All rights reserved

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

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

Online Editor Daniel Shepherd daniel.shepherd@cpimediagroup.com

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com

### ENTRUST AND STARLINK ANNOUNCE STRATEGIC PARTNERSHIP TO BOLSTER DIGITAL SECURITY OFFERINGS IN THE MIDDLE EAST & AFRICA

#### Entrust, a global leader in trusted

identity, payments and data protection, has partnered with StarLink, an Infinigate Group company and a regional leader in cyber and cloud solutions, with the aim of providing cutting-edge digital security solutions to organisations in the Middle East and Africa region.

In line with regional efforts to combat looming cybersecurity threats, the two companies are on a mission to provide local customers with the highest standards of cyber security. The new partnership will see StarLink becoming Entrust's newest distribution partner for the Middle East and Africa region, providing customers access to the full range of Entrust's certificate solutions, PKI, identity and access management, encryption key management and hardware security modules.

The partnership was inked during an MoU signing which took place on the sidelines of GITEX Global 2023 in the presence of Simon Taylor, Entrust MEA Channel Director, Alaa Abdo, Vice President of StarLink, and Julien Caifero, Director of Global Business Development at Infinigate.

Simon Taylor, Channel Director, MEA



at Entrust, said: "The ongoing digital transformation across all sectors is bound to be coupled with a simultaneous increase in cyberattacks which will continue to increase in sophistication. In light of this, we are delighted to announce our new strategic partnership with StarLink. Together, we aim to strengthen the digital security posture of companies in the region and help them defend against an ever-evolving threat landscape. This partnership is a testament to our solid commitment to better serve our existing and potential customers in the region."

Julien Caifero, Director – Global Business

Development, Infinigate (representing StarLink) said: "StarLink's mission is to reshape the distribution landscape by embracing disruptive and innovative approaches. Through this new partnership with Entrust, we are excited to provide them with regional on-ground support, extensive channel networks, and an unparalleled Go-to-Market (GTM) strategy, all of which will further develop and scale their business in the region. We're excited about the crossselling opportunities with complementary technology vendors that this partnership brings, and we look forward to expanding our cybersecurity offerings in the MEA region."

### TENABLE STUDY REVEALS 40% OF CYBERATTACKS BREACH SAUDI ARABIAN ORGANISATIONS' DEFENCES

#### Tenable, the Exposure Management

company, highlighted that, of the cyberattacks Saudi Arabian organisations experienced in the last two years, 40% were successful. This forces security teams to focus time and efforts on reactively mitigating cyberattacks, rather than preventing them in the first instance. With 68% of Saudi organisations confident that their cybersecurity practices are capable of successfully reducing the organisation's risk exposure, there is work to be done. These findings are based on a commissioned survey of 50 Saudi-based cybersecurity and IT leaders conducted in 2023 by Forrester Consulting on behalf of Tenable.

Respondents were particularly concerned with the risks associated with cloud infrastructure, given the complexity it introduces in trying to correlate user and system identities, access and entitlement data. Half of organisations (56%) say they use multi-cloud and/or hybrid cloud environments. However, over half of respondents (62%) cite cloud infrastructure as one of the highest areas of risk exposure in their organisation.



In order, the highest perceived risks come from the use of public cloud infrastructure (28%), multi cloud and/ or hybrid cloud (20%) and private cloud infrastructure (14%).

### VEEAM BROADENS DATA PROTECTION AND RANSOMWARE RECOVERY CAPABILITIES FOR MICROSOFT 365

#### Veeam Software, the #1 leader by

market share in Data Protection and Ransomware Recovery, announced that it has expanded its relationship with Microsoft. Veeam is making it easier for customers to protect Microsoft 365 with Cirrus by Veeam which brings the ease and flexibility of Backup-as-a-Service (BaaS) for Microsoft 365. Utilizing the power and reliability of the industry leading Veeam Backup for Microsoft 365 and our track record and experience with close to 18 million Microsoft 365 users under protection, these new BaaS capabilities, will include support for Microsoft 365 Backup Storage to give Microsoft customers the industry's most popular data protection and ransomware recovery capabilities.

"Businesses today need the confidence

that their critical business data is protected," said Danny Allan, CTO at Veeam. "We're delighted to extend the advanced capabilities we use to protect close to 18 million Microsoft 365 users by integrating with Microsoft 365 Backup Storage. The recent addition of our BaaS offering for Microsoft 365 underlines our commitment to continuing to deliver new features and capabilities that take advantage of the power and reliability of the Veeam Data Platform which keeps businesses running."

Veeam recently previewed this new integration with Microsoft 365 Backup Storage at Microsoft Ignite. The live demo highlighted the potential to quickly and efficiently restore large amounts of Microsoft 365 data, enabling organizations to minimize downtime following a ransomware attack or other data loss threat.



"Microsoft 365 Backup Storage provides high-speed point-in-time recovery for data stored in Microsoft 365 environments so customers can react and respond to the latest cybersecurity threats confidently," said Richard Riley, General Manager, Low Code and Content Services, Microsoft. "Integration with Veeam Backup for Microsoft 365 delivers our joint customers radical resilience with fast backup and restore of critical business data to keep Microsoft 365 users productive."

### HUAWEI DEMONSTRATES CYBERSECURITY LEADERSHIP AT ARAB INTERNATIONAL CYBERSECURITY SUMMIT 2023

#### At the recently concluded

2nd annual Arab International Cybersecurity Summit (AICS), Huawei showcased its cybersecurity assurance framework along with cutting-edge solutions and innovations with built-in security features while urging Middle Eastern leaders to reinforce cyber resilience through open collaboration. Participating under the theme "Security, No Compromise, Your Advantage, Security," Huawei was an official Telecom Partner at AICS 2023.

Held under the patronage of His Royal Highness Prince Salman bin Hamad Al Khalifa, Crown Prince, Deputy Supreme Commander of the Armed Forces, and Prime Minister of Bahrain, the Arab International Cybersecurity Summit 2023 was hosted by the National Cyber Security Centre (NCSC) and brought



together government regulators, industry professionals, and solution providers to discuss and develop plans to secure their cyber and IT infrastructure.

Aziz Tang, CEO, Huawei Bahrain, stated, "As a global ICT leader with a long-standing history in Bahrain and the rest of the Arab world, cybersecurity and privacy protection is our top priority. Customer trust and success are the foundation of our business, and we strive to live by this principle in every aspect of our business. The Arab International Cybersecurity Summit is the largest convention of its kind, and we are proud to demonstrate our cybersecurity leadership at this event."

Shaikh Salman bin Mohammed bin Abdulla Al Khalifa, CEO of NCSC Bahrain, visited the Huawei booth at the event and was briefed by Sultan Mahmood Malik, Cybersecurity and

Privacy Protection Office, Huawei Gulf North, on Huawei's latest cybersecurity innovations and its commitment to building a safer and secure digital economy in Bahrain. Shaikh Salman bin Mohammed bin Abdulla Al Khalifa felicitated Huawei in recognition of the company's efforts in helping build Bahrain's cybersecurity and pave the way for future collaboration and trust-building activities.

### WS02'S ASGARDEO SOFTWARE AS A SERVICE IDENTITY MANAGEMENT SOLUTION NOW AVAILABLE IN THE MICROSOFT AZURE MARKETPLACE

### WS02, the leader in digital

transformation technology, has announced the availability of Asgardeo Software as a Service Identity Management Solution in the Microsoft Azure Marketplace, an online store providing applications and services for use on Azure. WSO2 customers can now take advantage of the productive and trusted Azure cloud platform, with streamlined deployment and management.

WS02 Asgardeo supports all IAM use cases, which include Customer Identity & Access Management (CIAM) use cases like businesses engaging in B2B (Business-to-Business) and B2C (Business-to-Consumer). It also supports B2E (Business-to-Employee) interactions. Asgardeo for B2B offers a robust solution for ensuring secure access to your business products and services. It facilitates the seamless onboarding of users through the integration of enterprise internal developer platforms or by allowing customers and partners to self-register. Users have the flexibility to establish access policies that support multi-factor authentication, enhancing overall security. The implementation of role-based access control simplifies authorization management within your B2B applications by enabling the definition of user roles.

"WS02 Asgardeo facilitates secure and seamless collaboration between businesses by supporting standard identity federation protocols. It allows



businesses to establish trust and share resources securely with their partners," said Geethika Cooray, vice president and general manager of identity and access management at WSO2. "With WSO2's Asgardeo IAM solution running on Azure and available on the Azure Marketplace, development teams can now easily build, deploy and manage their cloud native applications with greater efficiency and agility," he added.

## HELP AG AND IMPERVA JOIN FORCES TO BOLSTER DATA AND APPLICATION SECURITY

#### Help AG, the cybersecurity arm of

e& enterprise and the Middle East's trusted security advisor, has joined forces with Imperva, the cybersecurity leader who protects critical applications, APIs and data, anywhere at scale. Help AG customers can now benefit from the Imperva Data Security Platform, to gain complete visibility into all data repositories, whether they are onpremises, in the cloud, or in hybrid environments. Help AG will also provide access to the market-leading Imperva Application Security products and solutions. The cloud-based services will be delivered through a local point of presence (PoP) in the United Arab Emirates. For organizations that seek robust security offerings that can accommodate the needs of developers and the ever-demanding DevOps landscape, Imperva products and solutions will be a good fit.

Today's customers require marketleading services, end-to-end solutions, and world-class technology expertise and guidance. Imperva and Help AG are joining forces to meet those customer needs, leveraging the Imperva Accelerate Partner Program to support this mutual success through a clear and well-structured framework, helping the partners maximize their value and extend it to clients.

The partnership is in line with Help AG's focus on integrated cybersecurity architecture, using Imperva's offering to strengthen zero trust and reinforce Help AG's leadership in the fields of data and application security.

Commenting on the partnership, Stephan Berner, Chief Executive Officer of Help AG, said: "At Help AG, we are dedicated to building strategic partnerships to constantly expand and enhance our 360-degree portfolio covering the entire lifecycle. Our partnership with Imperva supports



this objective, enabling our customers to secure their data at scale while ensuring compliance and unifying protection for applications, anywhere they run with the help of Imperva's advanced solutions."

Florian Malecki, VP – EMEA Channel Sales at Imperva, said: "Imperva Accelerate provides distinctive offerings that allow Help AG to build recurring revenue while assisting customers with establishing security programs that can scale and adapt to changing attack vectors. We are extremely pleased and excited by this partnership, and expect to accelerate our footprint with Help AG."



23-25 APR 2024 DUBAI WORLD TRADE CENTRE

# THE SUPER CONNECTOR EVENT FOR

936713 7173521

# **CYBERSECURITY** COMMUNITY

### **EMPOWER THE CYBER-SECURED FUTURE**

8143670502 7949970 49850259 57950876

#469247<del>02**12**1</del>47036

Enquire about Exhibiting, Sponsorship, **Speaking Opportunities & more!** 

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



SCAN HERE

#gisecglobal | gisec.ae

HOSTED BY

D TOTT

مجلس الأمن السيبراني CYBER SECURITY COUNCIL











OFFICIALLY SUPPORTED BY



ORGANISED BY



# TECHNOLOGY TRENDS AFFECTING THE SECURITY SECTOR IN 2024

JOHAN PAULSSON, CTO AT AXIS COMMUNICATIONS



ven for those of us who have been working in the technology industry for decades, the pace of change over the past 12 months has been extraordinary.

The key technological trends that we see affecting the security sector in 2024 reflect this rapidly evolving environment. As ever, they're a mix of positive opportunities to be grasped, alongside the challenges that need to be addressed.

### 1. Potential for generative AI in the security sector

In terms of AI, 2023 has been the year where large language models (LLMs) as the basis for generative AI have forced their way into public consciousness. This form of AI supports the creation of new content — words, images, even video based on natural language prompts and questions from users.

We do, of course, need to be aware of the risks and potential pitfalls of generative AI. There will be debates over



which models to employ and how, and particularly around the use of opensource vs proprietary models, but the biggest risk will be to ignore it.

### 2. Solution management efficiencies driving hybrid architecture

Hybrid solution architectures — those employing the advantages of on premise, cloud, and edge technologies — are now established as the new standard in many security solutions. Functionalities are deployed where it is most efficient, utilising the best of each instance in a system, adding an increased level of flexibility. Ultimately, system architectures should be in service to the customer's needs, not the vendor's preferred structure.

#### 3. Security always, but safety too

Security and safety have often been connected as a single subject. Increasingly they are being recognised as separate use cases: security being related to preventing intentional acts — break-ins, vandalism, aggression towards people, etc. — and safety related to the unintentional dangers and incidents that can cause harm to people, property, and the environment. Video surveillance will be used extensively within organisations to ensure adherence to H&S policies and safe working practices, such as the wearing of required Personal Protective Equipment (PPE). Where incidents do take place, video surveillance will be an increasingly useful and important tool in investigations. Security as a use case for surveillance is well-established. Safety will continue to evolve.

### 4. Regulation and compliance driving technology

Speaking of compliance, the global regulatory environment is having an increasing impact on the development of technology, its application, and use. Compliance with these is something that vendors and end users need to be aware of and should be looking to work in close partnership to ensure.

AI, cybersecurity, sustainability, corporate governance — all are areas coming under greater regulatory scrutiny. Vendors need to develop their own technologies and operate their own businesses in ways that support their customers' compliance requirements.

Increasingly, the regulatory landscape covers more than the specific

development and use of technology itself. Geopolitics and trade relations between nation states are also leading to regulations that demand transparency to a component level if vendors want to maintain a license to operate in key international markets.

#### 5. Taking the 'total system' perspective

The impact of every aspect of a security system will be under increased scrutiny, with vendors and customers needing to monitor, measure and, increasingly, report on a broad range of factors. Taking a total system perspective will be essential.

This total system perspective is useful and should be welcomed by the industry. It will lead to innovations in new technologies and cameras that bring benefits throughout the system, not in isolation. Cameras that reduce bitrate, storage, and server load with the intention of reducing server cooling requirements are a good example. More efficient transportation of products, sustainable packaging, and the use of standard components can all also play a part. Visibility and greater control across the supply chain is essential. **1** 



# LEADERSHIP DURING CRISIS

**FAYEZ IBBINI**, CEO OF ALPHA DATA, SPOKE TO SAME ABOUT THE RANSOMWARE ATTACK ATTEMPT ON HIS ORGANISATION IN JUNE, HOW THE PROCESSES THEY HAD PUT IN PLACE MITIGATED THE DAMAGE DONE, AND THE NEED FOR GREATER TRANSPARENCY AND OPENNESS WHEN IT COMES TO DEALING WITH RANSOMWARE ATTACKS. ayez Ibbini is one of the most respected and revered IT
 leaders across the Middle
 East.

The Jordanian national is a charismatic and dynamic force.

As the CEO of Alpha Data, he has helped nurture, guide and shape the organisation into one of the leading digital transformation providers and system integrator in the region over the last 40 years.

The company has naturally evolved over the years, and has pivoted to become a major player in digital transformation.

Over the last number of months his leadership mettle and skills have been put to the test, following a ransomware attack on Alpha Data in June, 2023.

An example of his resolute leadership has been the company's transparency over the attack which sent shockwaves through their organisation.

Rather than attempt to cover it up, or play the attack down, lbbini is using this interview to highlight what businesses can do to mitigate the damage caused by the inevitable ransomware that will hit them, whilst he is also hoping that by talking about their experience then that can change the 'stigma' around these types of attacks.

Ibbini highlighted that if companies are not properly prepared for an attack, then it could signal the death knell for their organisation.

"I really don't think people realise just how advanced these ransomware attacks have become. These are extremely sophisticated organisations that occupy large offices now, it is far removed from years ago when it was an individual hacker just trying his luck, and this is big business. When you're the victim of a ransomware attack you really do feel violated, and if you're not prepared for it then you may buckle from the intimidation tactics that are adopted by the hackers and pay the ransom fee they are seeking," said Ibbini.

Ibbini admitted that he was increasingly concerned that a ransomware attack was



becoming prevalent. With that in mind, in 2021, he hired a consultancy firm to do a stress test on the organisation and suggest enhancement to better protect the company against bad actors

"Two years prior to the attack, we hired a consultant to do a robust and thorough analysis on our vulnerabilities. We covered a lot of ground with them, but we discovered that the two components in which you can really become unstuck, was in relation to the fact that human beings are your biggest vulnerability, and secondly, it is imperative to have your data backed-up effectively. We weren't able to stop the ransomware attack, but the key learning for us from the consultation process was the fact that we started doing back-ups every six hours, and that really mitigated the impact of the ransomware attack. As I said I was fearful of an attack, you could say that I was paranoid about being hit by a ransomware attack after reading about so many international companies being attacked. Unfortunately, my worst fears came true. But the prior steps we had put in place by our security team and the consultancy firm allowed us to effectively respond without having to succumb to the demands of the hackers," said Ibbini.

Ibbini said that there remains a stigma

around these types of attacks, and has called for greater transparency.

He said there is a growing need for people to come together and share their experiences in order to create the knowledge that is required to be able to heighten awareness and enable businesses to respond.

"There is undoubtedly a stigma around being attacked, and I understand it's a difficult thing to accept, and as I said earlier you do feel violated. However, if we all try to keep it under wraps then we will only serve to further foster an environment in which we are all routinely attacked, and we don't learn from each other. In other areas and walks of life we share knowledge to create better awareness and improve things, so the same mindset needs to be adopted when it comes to ransomware attacks. We need open, candid and transparent conversations to really tackle this problem because it is not going to go away, we can bury our heads in the sands, but that's not going to achieve anything. I don't care what anyone thinks, and to be honest it was costly for us as an organisation to have been so transparent and publish the event on our website, but it was absolutely the right thing for us to do," said Ibbini.

### YOU DO NEED TO TRY AND PREPARE YOURSELF PSYCHOLOGICALLY BECAUSE THE ASSAULT IS → NOTHING LIKE YOU EXPECT, THESE PEOPLE HIT YOU HARD, AND THEY PREY ON YOUR VULNERABILITIES AND REALLY ATTEMPT TO INTIMIDATE YOU.

Ibbini reiterated his belief that it is not a case of if you get attacked, but instead when – and said it is nothing other than gross negligence for organisations to not be prepared for an attack.

"The first thing I want to stress is that everyone is vulnerable to a ransomware attack. Honestly, it's not a matter of if I get attacked, but instead when. The only reason that you haven't been attacked yet is because they are focusing on other targets, but at some point they will get around to you. If you live in the hope that they will not come to you then to be honest you are being so incredibly wishful period. When the day comes and you are hit, and you weren't prepared for it then vou have no excuse, and believe me if you're in business then your clients will never forgive you. If you don't present them with a strategy that you had in place to deal with an attack even if it failed.

then it is a serious breach of trust," said Ibbini.

"Ibbini said humans are always going to be weakest link in the chain, it doesn't matter how much you invest in education and training. To be honest, the best education is often the actual experience because the pain of it, and the disruption it causes really hammers home the seriousness of a ransomware attack, and the ramifications it can have on an organisation,"

The next piece of advice offered by Ibbini was the need for people to prepare, prepare and prepare.

"Even in the aftermath of our attack I am still thinking aspects we may have we potentially missed, where else are we potentially vulnerable? I never rest because ultimately, I am responsible for the company, our people, and our customers. You can't have an attitude of





look I've done my best, so let's move on, you constantly have to be looking at ways in which you can enhance the security of your operations," said Ibbini.

Ibbini also highlighted the importance of doing routine back-ups, but stressed that just doing back-ups wasn't enough and that businesses were guilty of neglecting the testing of the recovery from a real disaster.

"A big issue is around backup, either companies are guilty of not conducting back-ups frequently enough, or when they do back-ups, they never actually tested the recovery. If you don't test it then you don't know how reliable it is and defeats the purpose of the back-up in the first place. In addition to this, you need to determine how long you can live without your systems in place. If you lose a day of data is that too much, or is it 2 days, or 3 days, what is your limit? If you have a very high transaction business then a day is definitely too long. You also need to encrypt your critical data. They will get in and attempt to exfiltrate your data, but at least if the critical data is encrypted then it protects you to a certain degree," said lbbini.

Ibbini moved the dial of the conversation towards the psychological toll that such an attack can take on people due to the invasive nature of being hit by a ransomware attack and the intimidation that is deployed by the hackers.

"This is difficult, but you do need to try and prepare yourself psychologically because the assault is nothing like you expect, these people hit you hard, and they prey on your vulnerabilities and really intimidate you. They also can make it very personal and will attempt to target your family. For example, on the day of the attack my wife and 2 of my children got a call from one of the hackers in relation to the ransomware attack using voice altering technology. There's no limits to what level they will stoop to in order to intimidate and threaten you and it's a horrible situation to be in," said lbbini.

It has been well known that many businesses that have been hit by ransomware attacks have paid the ransom in order to get their data back, but Ibbini declared that you should never ever engage with the hackers, let alone consider paying the ransom. Even if you should pay, there is no guarantee of recovering your data or appearing as easy target and more repeat attack in the future.

"The hackers are clever and they know that time is not on their side, they have a short window of opportunity. When a company is hit those impacted are naturally confused and worried, so day one is when you are likely to pay the ransom, every night you sleep on it you are less likely to give in to their threats. So, they have to keep hitting you really hard in the first few days because they know if it goes beyond a certain point then the chances of them making money diminishes rapidly. The other thing I would stress is do not negotiate, engage, or connect with the hackers on any level at all. Never mind the negotiations, do

THERE IS UNDOUBTEDLY A STIGMA AROUND BEING ATTACKED, AND I UNDERSTAND IT'S A DIFFICULT THING TO ACCEPT AND THE VIOLATION YOU FEEL WHEN IT HAPPEN. not even answer an email said Ibbini.

Ibbini also highlighted the importance of ensuring your back up is not connected to a network.

"What we also discovered through this process was that you can get some sort of assurance from having a solid backup, but that back-up can't be connected to the network, we call it air-gapped. "When you back-up something it has to be disconnected, there should be no way to infiltrate the backup. Essentially, what this allowed us to do was recover our data and this frustrate the backers I used to receive emails every other day. but after June 20th, the volume of emails began to decline. Now you feel that hopefully they have gone away, but they won't go guietly. These are vindicative people and they will publish sensitive information and will do everything they can to harm because ultimately, they never got anything out of you," said Ibbini.

Ibbini said that the hardest part of the attack was reassuring clients that their data had not been compromised, and said the most important thing was to ensure business relationships are preserved.

"You need to be proactive with all your clients, and go and visit them and explain the situation. Our clients vary from mature and very sophisticated businesses to smaller enterprises. A sophisticated client will say to you that ' look we know these things happen, and we know how widespread an issue it is, but just do your best and keep us posted'. Some clients are not as an understanding, and may will actually block you. So, then you've got to go and do your homework and show them the steps, measures and processes that you took to safeguard their data. It takes a lot of cajoling, and convincing to get them back onside, and that is the hardest part about the whole thing, as much as recovering your data is tough, but the hardest part is making sure it doesn't fracture your business relationships," said Ibbini.

Ibbini concluded a wonderful discussion by highlighting that his



### THE OTHER THING I WOULD STRESS IS DO NOT NEGOTIATE, ENGAGE, OR CONNECT WITH THE HACKERS ON ANY LEVEL AT ALL.

motivation behind this article was to serve as an inspiration to others to come forward and share their ransomware experiences in order to really start having the conversations that need to happen to really enact change.

"Life teaches you that transparency isn't just a virtue, transparency saves you a lot of headaches. Lies will eventually trip you up, once you say it happened, then have taken the right first step to recovery, you are trying to rectify the situation, and are doing your best, and that is anyone can do.

I wanted to share our experiences to actually help businesses deal with being hit by a ransomware attack. We hear lots of theoretical advice about what you need to do to prevent it, but we need businesses to start actually talking more about real experiences , in order to enhance the knowledge that is required to ultimately really tackle this widespread issue. I am not lecturing to anyone on security, I go to conferences all the time and we hear advice on how to prevent it, but what everybody really wants to hear is how did you deal with it? In summary, what doesn't kill you makes you stronger. We are still here, we didn't lose anything, and the business is going from strengthto-strength – we can serve as hope to others that you can overcome these attacks, and be a stronger organisation at the end of it," said Ibbini. 1

### INSIGHT / KASPERSKY

# MIDDLE EAST REMAINS ONE OF THE REGIONS MOST TARGETED BY CYBERCRIME IN 2023

s organisations continue to become more digitised, throughout 2023 the Middle East remains one of the world regions most targeted by cybercrime. Kaspersky shared some insights and statistics related to the regional threat landscape in the third quarter of 2023 and made forecasts on how the situation is going to develop in 2024.

#### Phishing

Phishing is a type of Internet fraud that seeks to acquire a user's credentials by deception. It includes theft of passwords, credit card numbers, bank account details and other confidential information.

Phishing attacks on corporate users detected in the Middle East in Q3 2023 increased by 35% compared to Q2 2023; however, compared to Q3 2022, the number of phishing detects decreased by 7%.

#### **Attacks on Industrial Control Systems**

The Middle East is among the regions with the highest number of detected attacks on industrial control systems (ICS computers). ICS computers are used in energy and mining sectors, automotive manufacturing, building automation infrastructures and other spheres to perform a range of operational technology functions – from the workstations of engineers and operators to supervisory control and data acquisition servers.

In Q3 2023, according to Kaspersky ICS CERT, attacks were detected on 27% of ICS computers in the Middle East. Globally, malicious objects were detected on 25% of ICS machines in Q3 2023. All these attacks were blocked by Kaspersky solutions.

#### Attacks on the Internet of Things

The number of attacks on Internet of Things (IoT) devices has been increasing exponentially over the last years globally. This is related both to the activity of criminal actors and to the increasing number of IoT devices that are in use by individual users, businesses, and production facilities. IoT devices include not only wearables and smart home appliances, but also smart city systems, self-driving cars, automated retail checkouts, and other smart devices for home and business use. These devices can collect and transfer data over a wireless network without human input. Cybercriminals use networks of infected smart devices to conduct DDoS attacks or as a proxy for other types of malicious actions.



Kaspersky detected over 2 million attacks on IoT devices in the Middle East in Q3 2023. All these attacks were spotted on Kaspersky IoT honeypots – decoy devices used to attract the attention of cybercriminals and analyse their activities.

"In forecasting the development of the cyberthreat landscape for 2024, we anticipate a dynamic evolution of cyberthreats marked by an upsurge in state-sponsored cyber-attacks, and 'hacktivism' will become one of the norms of cyber-warfare," comments Dr. Amin Hasbini, Head of Kaspersky Global Research and Analysis team for the Middle East, Turkiye, Africa region. "Exploitation of vulnerabilities in mobile and IoT devices will be on the rise. The prevalence of accessible



generative AI is set to fuel an expansion of spear-phishing tactics and AI-assisted malware development, including through malicious AI bots, such as FraudGPT, WormGPT, and WolfGPT: they can create realistic phishing emails targeting employees to convince them into paying fraudulent invoices or help criminals develop malware much quicker for example."

"Businesses today should be proactive and counter these cyberthreats with advanced technologies such as threat feeds, security information and event management systems, endpoint detection and response solutions, and tools with digital forensics and incident response features," concludes Dr. Hasbini. cyberthreats, Kaspersky experts recommend:

- Organisations should conduct regular cyber skill checkups among employees and offer competent training. Kaspersky Security Awareness portfolio offers flexible ways to train staff, is easily customisable and scalable to meet the needs of any company size.
- Corporate users should be educated on potential privacy risks when working in virtual environments.
   Organisations should implement best practices in safeguarding personal and corporate data.
- Install updates for the firmware used on digital devices (including virtual headsets) as soon as they become available.

- Use Cyber Immune solutions for IoT protection on corporate networks.
   Use a dedicated IoT gateway that ensures inbuilt security and reliability of data transferring.
- Use Kaspersky Threat Intelligence to block network connections originating from malicious network addresses detected by security researchers.
- Establishing continuous vulnerability assessment and triage as a basement for effective vulnerability management process. Dedicated solutions like Kaspersky Industrial CyberSecurity may become an efficient assistant and a source of unique actionable information, not fully available in public.

To protect organisations from

# MEET FORTINET ADVISOR, A GENERATIVE AI ASSISTANT THAT ACCELERATES THREAT INVESTIGATION AND REMEDIATION



ortinet, the global cybersecurity leader driving the convergence of networking and security, has added Fortinet Advisor, a generative AI (GenAI) assistant, to its portfolio of more than 40 AI-powered offerings. AI has served as the backbone of the Fortinet Security Fabric and FortiGuard Labs threat intelligence and security services for more than a decade, and the implementation of GenAI is Fortinet's latest innovation designed to protect customers and keep business operations online. The initial release of Fortinet Advisor will help support and guide security operations (SecOps) teams so they can investigate and remediate threats faster than ever before.

"Fortinet has pioneered artificial intelligence innovation within cybersecurity, and to date, we've delivered more than 40 AI-powered offerings that put the transformative power of this technology into customers' hands," said Michael Xie, Founder, President, and Chief Technology Officer at Fortinet. "We're excited to build on our legacy as a leader in AI cybersecurity innovation with Fortinet Advisor, which combines Fortinet's vast intelligence network with the benefits of GenAI to increase security team productivity and accelerate threat detection and mitigation."

#### Fortinet Advisor Empowers SecOps Teams

Today, Fortinet Advisor is available within FortiSIEM, Fortinet's security information and event management solution, and FortiSOAR, Fortinet's security orchestration, automation, and response offering. Fortinet Security Operations Solutions already enable customers to slash the time needed to identify and contain threats from more than 20 days to less than an hour and condense investigation and remediation timelines from more than 18 hours to 15 minutes or less. By providing contextually aware incident analysis, remediation guidance, and playbook templates, Fortinet Advisor delivers critical information in natural language within seconds so SecOps teams can further reduce the mean time to detect and respond as well as improve their organisations' overall risk posture.

Specific benefits of Fortinet Advisor for SecOps teams include:

- Interprets security incidents: Fortinet Advisor rapidly analyses alerts to generate easy-tounderstand incident summaries within seconds, including context and potential impact.
- Builds complex investigation queries: Fortinet Advisor helps security analysts generate productive queries to aid investigations. Analysts enter their desired insights—in natural language—into Fortinet Advisor, which creates precise syntax to return useful results.
- **Creates remediation plans:** Fortinet Advisor aids in rapid threat response by suggesting threat remediation plans. It can also refine suggested response plans based on real-time analyst feedback.
- Augments playbook creation: Security architects can consult Fortinet Advisor to generate playbook templates, translating processes into actionable plans quickly.

Fortinet Advisor is continuously updated and refined by Fortinet AI and



product specialists. Fortinet experts regularly refresh the assistant's knowledge base with the latest threat information and optimize its interactions and results.

### More than a Decade of AI-Powered Threat Research, Prevention, Detection, and Response

Fortinet has been on the bleeding edge of Al innovation for more than a decade, and more than 700,000 customers already benefit from Al-powered offerings, including FortiGuard Al-Powered Security Services, FortiAlOps, FortiEDR, and FortiAnalyzer. The use of Al across the Fortinet Security Fabric aids in zero-day threat detection, helps remediate today's most sophisticated attacks, and enables IT teams to refine and resolve networking and security issues before they impact the organisation.

# $\rightarrow \begin{array}{l} \text{TODAY, FORTINET ADVISOR IS AVAILABLE WITHIN} \\ \text{FORTISIEM, FORTINET'S SECURITY INFORMATION} \\ \text{AND EVENT MANAGEMENT SOLUTION.} \end{array}$

#### An Industry-Leading Cybersecurity Platform

The Fortinet Security Operations portfolio is a part of Fortinet's cybersecurity platform—the Fortinet Security Fabric—and because of this tight integration, organisations can move from a reactive to a proactive security posture and quickly detect and disrupt cyberthreats. Fortinet Security Operations Solutions utilise AI and advanced analytics to identify sophisticated threats early in the kill chain and automate response activity across the Fortinet Security Fabric to speed investigation and remediation.

"GenAl has the power to make security teams smarter, more efficient, and more productive. Fortinet Advisor, which is backed by Fortinet's long history of Al innovation and deep threat expertise, can help organisations improve business operations and harden themselves against attack, especially for those struggling with the cybersecurity skills gap." – Jon Oltsik, Distinguished Analyst and Fellow at Enterprise Strategy Group. **1** 

# COMMITTED TO CYBERSECURITY

ANITA JOSEPH CAUGHT UP WITH **NED BALTAGI**, MANAGING DIRECTOR – MIDDLE EAST, TURKEY, AND AFRICA AT SANS INSTITUTE, TO FIND OUT MORE ABOUT CYBERSECURITY IN THE REGION AND HOW SANS IS COMMITTED TO EQUIPPING PROFESSIONALS WITH THE REQUIRED SKILLS.

> hat role does the SANS Institute play as a leading and dynamic thought leader in the cybersecurity sector, and how does its influence shape the

#### industry's landscape?

At SANS, we are committed to developing the next generation of cyber leaders globally. With more than 85 training courses that cover a broad spectrum of topics, ranging from foundational courses to highly specialized areas such as DFIR, OSINT and ICS, we are well-positioned to help companies overcome digital security and privacy challenges. Our courses are taught by experienced practitioners who bring realworld experience to the classroom, and training materials are continually updated to reflect the latest threats and vulnerabilities. Research by our faculty members into emerging threats and trends is shared with the cybersecurity community through publications and events, including webcasts, conferences, and summits. We maintain a strong focus on community building and networking, which fosters collaboration and knowledge-sharing among cybersecurity professionals. We are active advocates for a

strong cybersecurity culture within organisations and throughout the industry. Overall, our goal is to help organisations build more secure and resilient systems that can withstand the evolving threat landscape.

### What are the current cybersecurity trends in the UAE and the broader META region?

All through 2023, the world has witnessed a revolution in Artificial Intelligence (AI) and Machine Learning (ML). Notably, the cybersecurity industry has been actively and significantly involved in adapting to and leveraging these transformative advancements. Al and ML now play a crucial role in enhancing cybersecurity measures within organizations in the UAE and Middle East, by automating tasks and eliminating manual processes across operations, enabling the prevention of potential risks evolving into security incidents and fundamentally reshaping how professionals address digital security. Moving forward, we can expect an even greater reliance on AI and ML to detect and mitigate threats in real-time.

Additionally, the shift to cloud environments in the META region is gaining momentum, and



with this new frontier for cyber threats comes the need for a robust cloud security strategy. Businesses in the Middle East have invested in securing their assets, data, and operations in the cloud, deploying identity and access management, encryption, and multicloud security solutions. Moreover, cloud security professionals in the region have already recognised Zero Trust as the top priority in cloud security for 2024.

CISOs acknowledge that, despite significant investments in cybersecurity and cloud security solutions, the potential for human error, such as an employee accidentally opening a phishing link or providing unauthorised access, remains a significant vulnerability. This realisation underscores the heightened importance of adopting Zero Trust security models to mitigate the risk of both internal and external breaches.

The Middle East places heavy emphasis on cyber resilience. This extends beyond mere attack prevention, centering on how businesses can maintain seamless operations even in the event of a breach – minimising disruptions during the attack and facilitating prompt recovery afterward. The UAE's implementation of comprehensive cybersecurity certifications, standards, and policies exemplifies the region's commitment to maintaining robust cyber resilience across various sectors.

WE AIM TO ORGANISE AS MANY TRAINING EVENTS PER YEAR AS POSSIBLE FOR THE REGION, BRINGING → OUR EXPERT INSTRUCTORS OVER TO UPSKILL LOCAL CYBERSECURITY PRACTITIONERS.





### Tell us more about the Middle East threat landscape in 2023 & 2024. What specific skills do professionals in the region need to overcome threats and bridge the skills gap?

The Middle East's cybersecurity threat landscape in 2023 and 2024 is characterised by its dynamic and challenging nature. Professionals in the region need to equip themselves with a range of specific skills to effectively navigate and mitigate these threats everything from advanced threat detection to cyber resilience planning. We have been working closely with different government entities across many nations in the META region, as well as globally, on setting up programs that help narrow the cybersecurity skills gap. One of the largest training gaps in the region is in ICS cybersecurity. Critical infrastructure in Oil & Gas is a major part of operations in the Middle

East, and IT security training, tools, practices, and processes do not always translate well into control systems. In many cases, it actually causes more problems. 38% of attacks in ICS critical infrastructure networks come from IT networks allowing the threats into the ICS. As such, there is an opportunity to connect with professionals, educate them on ICS threats, and offer training courses such as ICS515, ICS418, and ICS410.

### Will there be more SANS META region training events in 2024? What can cybersecurity professionals look forward to?

Over the years, the number of training events we host in the region has grown by good measure, and we are excited that the META region in 2024 will be hosting more than 15 training events. We aim to organise as many training events per year as possible for the region, bringing our expert instructors over to upskill local cybersecurity practitioners where possible. We will be hosting training in the UAE, Saudi Arabia, Oman, Kuwait, Qatar, and Turkey with a variety of training courses covering the latest trends and techniques in cybersecurity, hands-on exercises and insights, and networking opportunities within the cybersecurity community, providing valuable experiences for professionals in the field.

The SANS META region training events in 2024 are not just educational opportunities; they are comprehensive experiences designed to elevate the skills and strategic thinking of cybersecurity professionals in the Middle East. These events represent our ongoing dedication to nurturing a knowledgeable, resilient, and collaborative cybersecurity community in the region.

# IT SECURITY PREDICTIONS FOR 2024 -CLOUDFLARE GRANT BOURZIKAS, CSO CLOUDFLARE

- 1. The knowledge gap between security professionals who understand AI and those who do not will be the number one reason for any shift in the balance of power to threat actors. Whether or not the usage of Al is giving attackers a leg up is the wrong question to be asking. Al is here to stay, so the right question is whether or not security leaders possess the skills required or will invest the time to upskill and learn how to handle what is becoming the largest revolution ever seen in technology. Both harnessing the power of this technology and defending against it, hinges on the ability to connect the conceptual to the tangible. If the security industry fails to demystify AI and its potential malicious use cases, 2024 will be a field day for threat actors.
- 2. The AI arms race will officially commence, and the first AI model breach will take place. Organisations of all types are aggressively adopting and beginning to rely on models to carry out critical business functions. Moreover, organisations are leaning heavily on AI to maintain a competitive edge, with Wall Street upgrading the stocks of companies that mention AI and punishing those who are seemingly behind the technology curve. As with any technology that becomes a crucial piece to an organisation's success, it increasingly becomes a top target for threat actors to inflict significant damage. Organisations rushing to join this revolution without the proper precautions put in place are opening themselves up as a low hanging fruit for model tampering and breaches - ones that could have the power to impact everything from critical care,
- The only way to fight against AI is with Al... if you have already mastered the basics. Defending against AI ultimately means defending

banking systems, power grids etc.



against all human knowledge indexed. Information sharing exists at an order of magnitude faster, and is more efficiently exchanged than ever before. Security pros protecting their organisations in the era of infinite information face challenges never seen before. But if the industry has historically struggled with doing the simple things well, over pivoting to solve issues using Al will be mostly benign. Sometimes the best way to mitigate attacks is by going back to foundational elements of detection and mitigation.

4. The next cutting-edge security technology that will hit the market in 2024 will be the ability to identify and eliminate the usage of deep fakes on social media and in modern media. One of the main goals of a threat actor is to erode trust, and one of the most useful tools to achieve this is by leveraging deep fakes. While deep fakes have been around for years, today's versions are more realistic than ever. Untrained eyes and ears cannot discern what is fake... and with today's versions more realistic than ever, trained eyes and ears also fail to identify deep fakes.

5. The number one focus for customers in 2024 will be around achieving resilience. The Internet has become a pillar of critical infrastructure, and this year will become more dangerous than ever. In 2024 the number one concern of our customers will be resilience. As more zero-days, flaws in popular software, supply chain issues and threat actor tactics evolve and come to fruition, organisations are hyper vigilant on the steps they can take to remain protected. Responsible disclosure will be a critical pillar in upholding resilience – no matter the priorities or style of the CISO. Managing incidents like zero-days isn't as simple as "run the patch, now you're done." In 2024. security leaders will begin the mindset shift towards turning incident management, patching, and evolving security protections into ongoing processes. Mitigations like patches for each variant of a vulnerability may reduce your risk, but they never fully eliminate it. 🚺

# POSITIVE TECHNOLOGIES: SUCCESSFUL CYBERATTACKS ON FINANCIAL ORGANISATIONS HAVE DOUBLED

ositive Technologies, an industry leader in resultdriven cybersecurity, has analysed cyberthreats relevant to the financial

sector. Unique attacks on this industry doubled in Q3 2023 compared to the same period last year. Attackers primarily targeted the least secure organisations and their customers, most often with the help of malware. The percentage of encryption malware in such incidents increased 3.5 times. In addition, hackers are now more likely to exploit vulnerabilities on the network perimeter and compromise financial companies by attacking their supply chains. The databases and credentials obtained in such attacks are sold on cybercriminal platforms. At the same time, financial institutions continue to be targeted by hacktivists.

In the first nine months of 2023, most attacks (35%) involved malware. Encryption malware was used in 63% of incidents, while a year earlier it accounted for only 18%. The percentage of social engineering among the attack methods dropped from 47% to 25%. Positive Technologies attributes this to the growing popularity of other attack methods.

Analysts noticed a significant increase in incidents that exploited vulnerabilities on the network perimeter (32% of cases). There was also a significant percentage of incidents (22%) where organisations were compromised via their supply chains. Oftentimes, open-source software was used in such incidents to distribute malicious code. In one attack, the cybercriminals even created a fake LinkedIn page where they impersonated an employee of the targeted bank to conceal spoofing. Positive Technologies believes that such attacks may see a rise in popularity in the next few years, given the widespread use of opensource software by companies, including financial organisations, in their in-house software development projects.

Positive Technologies recommends that financial companies monitor the use of third-party components when developing their own software and check them for backdoors and vulnerabilities.

"Our research reveals that companies around the world have extremely low network perimeter security," Evgeny Gnedin, Head of Security Analytics at Positive Technologies, commented. "This was confirmed by penetration tests conducted by our experts for financial institutions in 2023. Our pentesters were able to gain access to corporate local area networks of all customer organisations by exploiting vulnerabilities in Internet-connected software. Only one bank tested had a good security system, but pentesters still managed to find and exploit a zeroday vulnerability. This proves that a motivated attacker can penetrate the IT infrastructure of even relatively wellprotected banks. Therefore, financial companies need to build security systems that will prevent non-tolerable damage to their business even if a hacker launches a successful attack."

Data leaks continued to be the most common attack consequence, rising from 51% to 64%. Among all malicious ads in the dark web and on dedicated Telegram channels and chats,



database-related messages accounted for 42%. In 43% of them, files were distributed for free: this is how hackers tend to punish companies for refusing to pay ransom. Ads selling fresh data and insider services amounted to 30%. Half of the databases under analysis had a maximum price tag of one thousand dollars, with one data row selling for about five dollars. Messages of database buyers accounted for 29%. Positive Technologies explains this high percentage by the fact that attackers are targeting specific organizations. In the financial sector, targeted attacks account for 98% of all incidents.

About 40% of the incidents involved disruptions in the availability of financial

services, mostly caused by ransomware attacks. This malware type was used in 63% of successful attacks. Some systems were shut down as a result of hacktivist attacks. Such incidents are typical for regions experiencing geopolitical tensions.

"Hacktivists attack individual companies, with the ultimate goal of destabilizing the country's entire financial system," said Artem Sychev, Advisor to CEO at Positive Technologies. "Attackers hope to spread panic among citizens and make them distrust financial institutions and the government. In this environment, financial companies should build their cybersecurity systems in such a way

POSITIVE TECHNOLOGIES RECOMMENDS THAT FINANCIAL COMPANIES MONITOR THE USE OF THIRD-PARTY COMPONENTS WHEN DEVELOPING THEIR OWN SOFTWARE. that prevents non-tolerable events from happening. This will ensure high operational reliability."

Mr. Sychev also highlighted the need for a centralized approach in addressing the growing cybersecurity challenges. This approach should include a coordinated response to threats at the industry level, as well as an analysis of possible chains of events that could lead to fatal consequences.

To mitigate cyber threats, the financial sector is recommended to use up-todate security tools, such as solutions for monitoring cybersecurity events and detecting incidents (MaxPatrol SIEM), endpoint security systems that protect against sophisticated and targeted attacks, effective vulnerability detection and management tools (MaxPatrol VM), fully automated result-driven cybersecurity solutions, and sandboxes that offer flexible customization of virtual environments to facilitate analysis and detect threats in files and network traffic (PT Sandbox). **1** 

# PHYSICAL SECURITY MARKET TO EMBRACE CLOUD AND HYBRID SOLUTIONS: GENETEC 2024 STATE OF PHYSICAL SECURITY REPORT

FOR OVER 25 YEARS, GENETEC, A GLOBAL TECHNOLOGY COMPANY, HAS BEEN AT THE FOREFRONT OF REVOLUTIONISING THE PHYSICAL SECURITY INDUSTRY. TODAY, AI-DRIVEN ANALYTICS AND AUTOMATION ARE FUNDAMENTALLY RESHAPING SECURITY OPERATIONS, SIGNALING A TRANSFORMATIVE FUTURE FOR THE VIDEO SURVEILLANCE INDUSTRY. WE SPOKE TO **FIRAS JADALLA**, REGIONAL DIRECTOR – MIDDLE EAST, TURKEY & AFRICA, GENETEC, WHO SHED FURTHER LIGHT ON THE FUTURE OF THE INDUSTRY AND THE LATEST FINDINGS FROM THE COMPANY'S 2024 STATE OF PHYSICAL SECURITY REPORT.

### ow has the demand for video surveillance products changed in recent years, and what trends do you foresee in the near future?

The demand for video surveillance products in the Middle East has witnessed a significant uptick, driven by a growing emphasis on security and the rapid adoption of smart city initiatives. As urbanisation and infrastructure development surge, there's an increased need for advanced video surveillance solutions to safeguard public spaces and critical infrastructure. Additionally, the integration of video analytics and Al-driven capabilities has become more prevalent, enhancing the overall effectiveness of surveillance systems.

Looking ahead, the market is likely to see a continued focus on technological advancements, with a surge in demand for high-resolution cameras, intelligent video analytics, and cloud-based solutions. In fact, our 2024 State of Physical Security Report, a study based on insights from over 5,500 physical security leaders worldwide (including end users and channel partners), revealed that physical security market is rapidly embracing cloud and hybrid solutions.



Privacy concerns is another area that is expected to influence the adoption of privacy-centric technologies, striking a balance between security and individual rights. The convergence of video surveillance with other smart city components, such as access control and IoT devices, will likely be a key trend, fostering more holistic and integrated security ecosystems.

### What makes your cybersecurity approach stand out in a market like the UAE?

The UAE's strategic role as a global business hub highlights the crucial need for robust cybersecurity measures to protect businesses, government entities, and individuals from today's fast-evolving cyber threats. With a rapidly advancing digital landscape, safeguarding sensitive data, critical infrastructure, and personal information has become imperative. As the country continues its digital transformation journey, a proactive approach to cybersecurity is vital for ensuring digital assets' integrity, confidentiality, and availability.

Recognising the paramount importance of cybersecurity, at Genetec, we prioritise safeguarding our customers' physical security systems from potential vulnerabilities. Our distinctive edge lies in the utilisation of the advanced Genetec Security Center platform, a robust solution designed to fortify devices against potential cyber threats. This platform unifies diverse security systems and data into a single interface, ensuring genuine integration and streamlined operations. Our commitment extends to maintaining the resilience of our systems through robust encryption protocols, regular software updates, and diligent provision of patches to address emerging security risks.

Furthermore, our cybersecurity strategy encompasses best practices for network segmentation, access control, and authentication. By adhering to industry standards and collaborating with cybersecurity experts, we ensure that our solutions remain at the forefront of resilience against cyber threats. This holistic approach provides our clients with the confidence that their critical security infrastructure is not only secure but also well-protected against the dynamic landscape of cybersecurity challenges.

### Security and privacy concerns are paramount in the video surveillance industry. How does your company address these concerns, and what measures do you take to ensure data

protection and user privacy? At Genetec, we firmly believe that security and privacy are not mutually exclusive. Our approach centers on responsible data gathering and management, especially in the realm of video surveillance, all while ensuring compliance with global privacy laws. Privacy by Design principles guide our innovative development, embedding privacy into our products from code inception to third-party integrations. One prime example is KiwiVision™ Privacy Protector™, seamlessly integrated into our Genetec Security Center platform. This tool automatically obscures individuals within a camera's view, safeguarding their identity and ensuring security operators only access pertinent information. To further uphold privacy, our solutions align with international standards like GDPR, CCPA, PIPEDA, and LGPD. Our commitment extends to data integrity, restricting access to authorised users and empowering end-users to configure systems to their privacy preferences. Just as a homeowner controls access to their residence, we, as software manufacturers, share the responsibility of providing robust tools that prioritise privacy without compromising security. Our holistic approach places user control at the forefront, offering a transparent and configurable system that respects individuals' privacy rights while ensuring optimal security measures.



### How do you customise your security solutions to meet the unique challenges and requirements of businesses in the UAE?

Customising security solutions for businesses in the UAE is a collaborative process that hinges on understanding each customer's unique needs. With many enterprise clients having sophisticated requirements, we closely collaborate to develop tailored features within our products. Recognising that security teams often underutilise their



systems, we address the consumption gap by working with systems integrators. Beyond initial deployment, we assist in bridging this gap through training plans, ensuring customers maximise the full potential of their security investments. This approach not only enhances the effectiveness of current systems but also creates opportunities for future growth and expansion of services, fostering long-term customer satisfaction and engagement.

### How do you envision the future of video surveillance technology, and what new developments can we expect from Genetec in the coming months?

The future of video surveillance is poised for transformative advancements, and at Genetec, we're at the forefront of pioneering innovations. We foresee a landscape where Al-driven analytics and automation redefine security operations, enhancing both efficiency and effectiveness. Genetec is committed to pushing these boundaries, introducing cutting-edge developments in the coming months.

As we navigate the dynamic landscape of security technology, Genetec is poised to introduce solutions that not only meet the challenges of today but also anticipate the needs of tomorrow, setting new benchmarks for the industry. Stay tuned for a future where video surveillance is not just a tool but a strategic asset in ensuring the safety and security of communities and organisations.

# TRELLIX RELEASES MINDOF THE CISO REPORT

ll UAE-based security leaders who have lived through a recent cyber incident believe that future prevention hinges on the training of people, and improvements in technology, and almost all (96%) want to see similar enhancements in processes. These critical findings emerged from research released from Trellix, as part of the company's Mind of the CISO initiative. The report, titled "Mind of the CISO: Behind the Breach" was designed to better understand the unique challenges faced by CISOs and other high level security decision makers, in the aftermath of a cyber-attack.

Some of the key findings in the research focused on the extent to which gaps in people, technology and process contributed to a major cyber incident. In terms of people-readiness, 64% of respondents from the UAE said the incident was missed because of a lack of resources (for example, it may have occurred in off-shift hours). More than half (52%) of those polled said their organisation lacked the IT skills to deal with the complexity of the incident.

In terms of impact of technology gaps, 52% cited gaps in security capability as a contributor to a security incident and 44% said their IT stack was not configured correctly or that detection policies were not enabled. Some 40% said that their IT and security tools did not provide adequate visibility to stop an incursion.

In a ripple effect, tech gaps, according to the poll, were leading to collapses in

processes, with 52% saying workflows could not be fully executed because the tools were not in place to allow it. Almost half (48%) said their organisation used too many manual processes, which had a negative impact on the mean time to detect (MTTD) or repair (MTTR). And 44% cited a lack of properly documented and implemented processes while another 44% decried the lack of context arising from disconnected security controls.

The report revealed that post-breach analysis by UAE security leaders had, on average, concluded that change was necessary to prevent repeat occurrences. Sixty per cent of those surveyed said their organisation's experience during the incident had caused it to completely rethink its cybersecurity strategy. Almost all respondents (96%) agreed



that some improvements were needed in their processes. And all agreed their organisation had to make some improvements in terms of people and technology.

"Once again, we see the challenges faced by the UAE's cybersecurity professionals," said Vibin Shaju, General Manager, UAE at Trellix. "What is clear from what interviewees told us is that people, processes, and tech are three legs of stool. If you overemphasise one, the stool becomes wobbly and can topple. There must be balance. What we see in our survey are real-world examples of those who had wobbly stools, and what it cost them."

In the context of their cyber incident, respondents were polled on the benefits of extended detection and response (XDR), the emerging approach in cybersecurity that brings together disparate security tools in a powerful single-pane solution. Some 72% cited faster and more efficient threat detection and response. Among those respondents that did not have XDR deployed at the time of their incident, all agreed that the technology would have at least lessened the impact of the breach, and almost all (91%) believed it would have prevented the incident altogether.

"XDR is one of the best cybersecurity investments available today," continued Shaju. "It offers improved, consolidated visibility by ingesting data from siloed security solutions. It offers automated analysis that yields insights that would be unlikely to emerge from manual processes. The security function is therefore empowered to carry out faster, more productive investigations because the platform has already prioritised avenues of inquiry. Here we can see an end to alert fatigue and the beginning of a new era of high morale in the SOC and less risk across the board. And if that is not enough to get security leaders thinking in a new direction, imagine making a business case for XDR in which you can say with confidence that the entire security stack, now consolidated and simplified, will have a lower total cost of ownership."

"Every day our security professionals are under siege. Our 'Mind of the CISO' reports show this, not in theory but in fact. XDR lifts them up and lets them take the fight to the threat actor," concluded Shaju.

# KYNDRYL COLLABORATES WITH MICROSOFT, RELEASES GLOBAL SUSTAINABILITY BAROMETER STUDY



yndryl, the world's largest IT infrastructure services provider, in collaboration with Microsoft, has released the findings of The Global Sustainability Barometer study. The study, conducted by Ecosystm, finds that while 88% of organisations in the United Arab Emirates (UAE) place a high strategic level of importance on achieving their sustainability goals, only 22% have integrated sustainability into their strategies and data.

As the world faces an increase in climate-related events and challenges, there is an urgency among businesses to act now using technology to drive sustainable solutions. While 63% of organisations surveyed in the UAE see great significance in technology's role to achieve their goals, only 30% believe they are making full use of it in their organisations.

"Many companies are at different stages of sustainability maturity," said Faith Taylor, Chief Sustainability and ESG Officer, Kyndryl. "Companies are applying technology to unlock the full potential of sustainability. They are thinking beyond regulatory compliance to pragmatically execute and advance their sustainability goals."

"Technology has emerged as a key

enabler to sustainability success, and its role will only continue to grow with the advent of more sophisticated AI tools," said Shelly Blackburn, Vice President, Cross Solutions Area, Microsoft. "We are eager to help drive meaningful change and contribute to a more sustainable future in collaboration with Kyndryl."

Key highlights of the survey include:

- While CEOs and boards have made sustainability and digital transformation a priority, they need help with integration and execution of their programs to meet their goals.
- 73% of organisations in the UAE use AI to monitor energy use, but only 46% use current data to predict future energy consumption.
- Among stakeholders of organisations in the UAE, employees are the most vocal in advocating for sustainability policies and practices, followed by investors, customers and government regulators.

### Drivers to Building a More Sustainable Organization in the UAE

Below are sustainability best practices for driving growth and improving business outcomes:

- Make sustainability a CEO and Boardroom priority aligned with finance and technology. Over 52% of organisations in the UAE entrust the CEO and the Board with leadership roles in their sustainability functions.
- Align sustainability with technology modernisation. Technology can help to automate, modernise and prioritise sustainability processes and infrastructures.



Of the respondents surveyed in the UAE, 64% use automation to improve efficiencies and build sustainable operations, while 51% use technology to reduce the environment footprint of their organisation and support data and reporting requirements.Build an integrated data foundation. Streamline data management for informed decision-making and successful execution of strategies. A mere 12% of organisations in the UAE have the capability to provide their employees with real-time sustainability dashboards.

- Unleash AI for predictive sustainability. Expand the use of AI beyond reporting to include predictive analytics that assess Scope 3 risks, forecast energy consumption and anticipate potential risks such as natural disasters.
- Empower employees. The study

# THERE IS AN URGENCY AMONG BUSINESSES TO ACT NOW USING TECHNOLOGY TO DRIVE SUSTAINABLE SOLUTIONS.

found that 55% of surveyed organisations in the UAE lack dedicated resources or limited internal expertise, which outlines the need for additional workforce development.

"Faced with record-breaking temperatures and unparalleled climaterelated events, this is a moment that calls for collective action from governments, industries, enterprises and individuals alike," said Ullrich Loeffler, Co-Founder & CEO, Ecosystm. "Together with Kyndryl and Microsoft, we are honored to make this study available to forward-thinking organisations everywhere to outline steps they can take today to drive measurable sustainability impact."

The Global Sustainability Barometer study, conducted by Ecosystm in collaboration with Kyndryl and Microsoft, was conducted among 1,523 technology and sustainability business leaders across 16 countries in Asia, Europe, Middle East and Africa (EMEA) and the Americas. The survey took place between September – October 2023. The survey was conducted across nine industries and included small to medium as well as global companies. Learn more about the study, "From Vision to Impact: The Global Sustainability Barometer."

### THREAT ACTOR TARGETS RECRUITERS THROUGH DIRECT EMAIL ATTACKS: PROOFPOINT

#### **Finance Director**

	<ul> <li>Annette Rawlings <ann@annetterawlings.com></ann@annetterawlings.com></li> </ul>	
0	То:	
Dear		

I am writing to express my interest in the Finance Director position at

I am confident that my background in finance and my proven track record in managing financial strategies make me a strong candidate for this role. To provide you with a comprehensive view of my professional qualifications and experiences, I have prepared an updated resume and additional materials which are available for review on my personal website.

I understand that including a direct link to my personal homepage may prevent this email from reaching you. Therefore, I kindly request that you refer to the domain name of my email address (ann@annetterawlings.com) to access to my professional portfolio and resume.

Thank you for considering my application. I am looking forward to the possibility of discussing my candidacy with you in more detail.

Warmest regards, Annette Rawlings

> ince at least October 2023, threat actor TA4557 began using a new technique of targeting recruiters with direct emails that ultimately

lead to malware delivery. The initial emails are benign and express interest in an open role. If the target replies, the attack chain commences.

Previously, throughout most of 2022 and 2023, TA4557 typically applied to existing open job listings purporting to be a job applicant. The actor included malicious URLs, or files containing malicious URLs, in the application. Notably, the URLs were not hyperlinked and the user would have to copy and paste the URL text to visit the website. The legitimate job hosting sites would then generate and send email notifications to the prospective employers who posted the positions.

In recently observed campaigns, TA4557 used both the new method of emailing recruiters directly as well as the older technique of applying to jobs posted on public job boards to commence the attack chain.

Specifically in the attack chain that uses the new direct email technique, once the recipient replies to the initial email, the actor was observed responding with a URL linking to an actor-controlled website posing as a candidate's resume. Alternatively, the actor was observed replying with a PDF or Word attachment containing instructions to visit the fake resume website.

Very notably, in campaigns in early November 2023, Proofpoint observed TA4557 direct the recipient to "refer to the domain name of my email address to access my portfolio" in the initial email instead of sending the resume website URL directly in a follow-up response. This is likely a further attempt to evade automated detection of suspicious domains.

Proofpoint has been tracking TA4557 since 2018 as a skilled, financially motivated threat actor. It is notably different from other priority threat actors tracked by Proofpoint due to the unique tool and malware usage, campaign targeting, use of job candidate-themed lures, sophisticated evasive measures employed to prevent detection, distinct attack chains, and the actor-controlled infrastructure.

Activity attributed to TA4557 has historically overlapped with activity associated to cybercrime group FIN6 by third parties in external reporting. The malware suite used by TA4557 has also been observed to be used by the cybercrime groups Cobalt Group and Evilnum, and Proofpoint tracks these as distinct activity clusters which are not often observed in Proofpoint threat data.

Today at 9:30 AM

TA4557 demonstrates sophisticated social engineering and tailors their lures to specific, legitimate job opportunities posted online. The tone and content of the emails suggest to the recipient the actor is a legitimate candidate, and because the actor specifically targets people who are involved in recruiting and hiring, the emails do not immediately seem suspicious.

Proofpoint has seen an increase in threat actors using benign messages to build trust and engage with a target before sending the malicious content, and TA4557 adopting this technique may convince recipients to be more trusting of the interaction and subsequent content shared with them. Additionally, the group is regularly changing their sender emails, fake resume domains, and infrastructure. This is done alongside building rapport with the target before sending a payload and poses a problem for defenders and automated security tools as it can be difficult to detect the content as malicious.

Organisations that use third-party job posting websites should be aware of this actor's tactics, techniques, and procedures (TTPs) and educate employees, especially those in recruiting and hiring functions, about this threat.

### معرض و مؤتمر الخليج العالمي لأمن المعلومات GSE GLOBAL 23 - 25 APRIL 2024 DUBAI WORLD TRADE CENTRE

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

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

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

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

HOSTED BY

01100

OFFICIAL GOVERNMENT CYBERSECURITY PARTNER





شرطة دبب DUBAI POLICE



ORGANISED BY

OFFICIALLY SUPPORTED BY





مركز حبات التجاري العالمات DUBAI WORLD TRADE CENTRE











GOLD SPONSOR

SCAN ME





**MI-F** 



### **BLAZING-FAST SPEED** No More Lag and Buffering



AX3000 Wi-Fi 6 Smart Mesh Router



works with Google Home

> AI WI-FI Optimizer

Al Mesh Optimizer

360° Spherical Coverage

> Get Started with AQUILA PRO AI App



Get IT ON Google Play



**AQUILA PRO AI**