

Security

ADVISOR

MIDDLE EAST

HIGHLIGHTS

DELL TECHNOLOGIES
ISSQUARED
42GEARS

NEXT-GEN CYBER DEFENCE

NED BALTAGI, MANAGING DIRECTOR – MIDDLE EAST AND AFRICA AT SANS INSTITUTE, TELLS ANITA JOSEPH, EDITOR, SECURITY ADVISOR MIDDLE EAST, THAT AS MORE AND MORE SKILLED WORKERS BECOME KEY TO DEFENDING MODERN ORGANISATIONS, THERE IS A RISE IN DEMAND FOR EQUIPPING PEOPLE WITH THE RIGHT KIND OF SKILL(S).

Empower **SMEs** With Digital

Helping Small- and Medium-sized Enterprises (SMEs) implement digital transformation
Huawei provides a range of product portfolios and solutions that can help enterprises to focus on their business growth and achieve their goals.

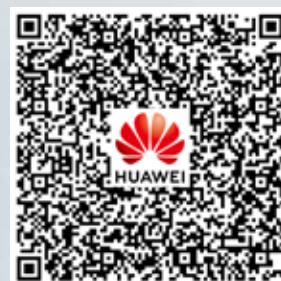
Available Products:

Campus Switches | WLAN | Access Routers | IdeaHub
OceanStor Data Storage | Data Center Switches
and more...

Stock Available, Delivery in 2 Weeks



Learn More



Contact Us



enterpriseME@huawei.com

e.huawei.com/ae



6 News roundup from the security industry in the region and beyond.

08 Anita Joseph, Editor, caught up with Jean-Guillaume (JG) Pons, Senior Vice-President of DELL Client Solutions Group (CSG), EMEA, to discuss how the company puts the customer at the heart of all its operations.

12 Werno Gevers of Mimecast on how threat actors refine attacks to cause devastating damage to organisations in Mimecast's latest State of Ransomware Readiness Report.

38 Mridul Ganguly, Head of Sales MEA at ISSQUARED, on how the company's key offerings enables customers to undergo a seamless digital and security transformation by being able to simplify, develop, build, and manage IT solutions for themselves.

Solar Powered Camera

No network cable required

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

Easy installation

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

Can withstand bad weather

Prone to extreme weather such as strong wind and rainstorms.



2MP
@ 30 fps



40W



20 Ah
lithium



4G



Beaufort scale **12**



IP67



Scan to Learn More



HIKVISIONMENA



HIKVISION-MENA



HIKVISIONMENA



HIKVISIONMENA

HIKVISION®

EDITOR'S NOTE



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

Anita Joseph
Editor

EVENTS



HITS & MISSES

2022 was a rough and tumble year, particularly for cybersecurity. Whether geopolitical tensions, or increasingly complicated ransomware attacks, targeted breaches and data thefts in the healthcare and education sectors, or even the various security trends that came, went or stayed, the past year left an indelible mark on the security market and served to doubly underscore the need for countries and businesses to invest in sophisticated cyber defence infrastructure at the earliest.

In this issue, we bring you exclusive insight and opinion pieces that highlight the various hits & misses in the security industry. We have experts and analysts discuss the trends that shaped the industry in 2022; we also have predictions for what is to come in 2023. Our cover story with Ned Baltagi of SANS Institute, for instance, throws light on the widening security skills gap and how the institute is stepping up with courses designed to bridge this space. According to him, there is an active and growing interest in cybersecurity and the need to address the shortage within the region, so there's that assurance that the gap is not being ignored as more organisations are investing in training

resources and both employees as well as employers are willing to bridge it by the day. Additionally, as more skilled workers are required to defend modern organisations, the demand is rapidly increasing to equip people who are new to cyber security, to support their organisations' cyber defense posture.

From skills to remote work-our focus interview this month with Jean-Guillaume (JG) Pons, Senior Vice-President of DELL Client Solutions Group (CSG), EMEA discusses how rapid digital transformation and the increasing propensity for remote work are necessitating a customer-first

approach and the need to customise solutions to cater to their varying demands.

Our other interviews spotlight the lessons learnt from the year that was and the roadmaps planned for the year to be. The regular Insight, News, Opinion, Spotlight and Perspective columns lay bare the milestones and misses of the security industry as it catapults into an uncertain, unpredictable future. In all, this is one issue you wouldn't want to miss, especially if you recognise and acknowledge the importance of a secure cyberspace.

So, here's wishing everyone a safe new year, Happy Reading!

UPS AND DOWNS FOR CYBERSECURITY

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by **CPI**

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

EDITORIAL
Editor
Anita Joseph
anita.joseph@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

© Copyright 2022 CPI
All rights reserved

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

SIMSPACE EXPANDS GLOBALLY WITH COMMERCIAL RELEASE OF CYBER FORCE PLATFORM

SimSpace, the industry leader in military-grade cyber ranges, has announced the commercial availability of its upgraded SimSpace

Cyber Force PlatformSM, expanding its footprint into a global market worth over \$200 billion.

During a period of unprecedented geopolitical risk, leading organizations can now use the same advanced technology as US national cyber defenders and global intelligence agencies. SimSpace can compress three years of attacks into 24 hours to ensure the highest levels of mission and defensive readiness.

The Russian war in Ukraine has fuelled a near 50% increase in cyberattacks in the first half of 2022. Goldman Sachs predicts a Russian attack on US infrastructure could cost the economy up to \$1 trillion. Businesses of national significance are seeking battle readiness for their cyber teams, and are using SimSpace's high-fidelity range capabilities to improve team and process performance, consolidate tools, and reduce costs.

The C-suite, board members, investors, shareholders, insurers, regulators, and audit committee members are grappling with the need for more concise quantifications of risk posture. Military-grade cyber ranges provide answers to those hard questions, and help businesses make \$30 million dollar decisions about changes in key parts of their cyber spending. SimSpace is trusted by the US Government, critical national infrastructure, F2000 organisations, and global intelligence agencies. By deploying the SimSpace Cyber Force Platform, organisations have achieved a 30% reduction in cyber operational costs and a 40% reduction in breaches in their production environments.



SOPHOS LAUNCHES INDUSTRY-FIRST MDR SERVICE FROM AN ENDPOINT SECURITY PROVIDER THAT INTEGRATES VENDOR AGNOSTIC TELEMETRY

Sophos, a global leader in innovating and delivering cybersecurity as a service, has announced the general availability of Sophos Managed Detection and Response (MDR) with new industry-first threat detection and response capabilities. Sophos is the first endpoint security provider to integrate vendor agnostic telemetry from third-party security technologies into its MDR offering, providing unprecedented visibility and detection across diverse operating environments. Sophos also introduced the Sophos Marketplace and \$1 million Sophos Breach Protection Warranty.

The need for MDR services and specialised defenders has never been greater, as shown in today's new research, "LockBit 3.0 'Black' Attacks and Leaks Reveal Wormable Capabilities and Tooling," from Sophos X-Ops, the company's cross-domain threat intelligence unit. The research analyses tactics, techniques and procedures (TTPs)

used by LockBit, one of today's most prolific ransomware gangs, that are similar to BlackMatter, and explains how the latest version of the ransomware, LockBit 3.0, adds wormable capabilities and uses legitimate pen-testing tools to evade detection.

In a second article, "Detection Tools and Human Analysis Lead to a Security Non-Event," Sophos X-Ops details a recent Sophos MDR use case involving credential theft, another technique that allows adversaries to impersonate legitimate users. In this case, the Sophos MDR team combined its threat hunting intelligence with information from the customer's third-party security appliance to thwart an attack.



RED HAT INTRODUCES LATEST VERSIONS OF RED HAT ENTERPRISE LINUX

Red Hat, Inc., the world's leading provider of open-source solutions, has introduced Red Hat Enterprise Linux 9.1, the latest version of the world's leading enterprise Linux platform. Along with the recently announced Red Hat Enterprise Linux 8.7, these minor versions add and refine capabilities for a wide range of enterprise IT needs, from helping to streamline complex infrastructure environments to improving the security stance of containerized applications.

Regardless of the environment, IT system security remains a constant concern for nearly every organisation. Red Hat Enterprise Linux 9.1 and 8.7 keep these needs front and center with operating system images that are pre-configured to meet organisation-specific system security needs. By enabling security compliance profiles in image builder blueprint files,

IT teams can specify an OpenSCAP security profile when extending Red Hat Enterprise Linux deployments with image builder to deliver operating system images that meet IT security and compliance requirements from installation.

Gunnar Hellekson, vice president and general manager, Red Hat Enterprise Linux, Red Hat said:

"As enterprise IT expands to encompass traditional hardware, multiple public cloud environments and edge devices, complexity grows in parallel. The latest versions of Red Hat Enterprise Linux continue our commitment to making hybrid cloud computing more than just accessible, but successful at the scale of global business by pairing reliability and stability with features designed for innovation and flexibility."



CLOUDFLARE INTRODUCES PROJECT SAFEKEEPING TO PROVIDE ZERO TRUST SECURITY FOR FREE TO CRITICAL INFRASTRUCTURE

Cloudflare, Inc. the security, performance, and reliability company helping to build a better Internet, has announced a new Impact Initiative to provide Zero Trust security at no cost to small and medium critical infrastructure organisations around the world. This new program, named Project Safekeeping, aims to protect under-resourced organisations that provide a critical community benefit but are at high risk for cyberattacks, with initial efforts focused in Australia, Germany, Japan, Portugal, and the United Kingdom.

"We know cyberattacks are on the rise and that critical infrastructure is a common target. But we know that when governments buckle down on security, that

often means the largest institutions are protected, at the expense of small communities," said Matthew Prince, co-founder and CEO, Cloudflare. "Given the success we've had with our critical infrastructure program in the United States, we're excited to bring it to more countries around the world. Cloudflare is the only company ensuring that Zero Trust is accessible to the smaller infrastructure organisations that are most vulnerable, and most relied upon in their communities – the local health clinics, energy providers, or local utilities that keep communities running."



AHAD LAUNCHES OFFENSIVE SECURITY UNIT (OSU) TO HELP PROTECT ORGANISATIONS FROM CYBER ATTACKS

AHAD, a cyber security and risk management company, has announced that it has launched an Offensive Security Unit (OSU) to help organisations protect their business from future cyber attacks before they happen. Most organisations are at risk of cyber-attacks, but few know how to prevent them. The Offensive Security Unit (OSU) is AHAD's answer to this problem. The unit will provide clients with a full suite of offensive security services, including penetration testing, red teaming, vulnerability management and adversary simulation that can help organisations identify and mitigate risky vulnerabilities before they are exploited by attackers.

"We believe that finding and fixing exploitable vulnerabilities with a well-strategised offensive security program is a critical component of an organisation's cyber defense strategy. The launch of our Offensive Security Unit (OSU) underscores our commitment to providing world-class cyber security services. We are dedicated to helping our clients protect themselves against the ever-growing threat of cyber-crime. In addition, we also provide consultation services for companies who find themselves under attack or want to prevent future cyberattacks against them. Our Offensive Security Unit will help clients protect their entire digital and physical ecosystem," said Ankit Satsangi, CTO, AHAD.



KASPERSKY PREDICTS SHIFTS IN THREAT LANDSCAPE TO INDUSTRIAL CONTROL SYSTEMS IN 2023

Kaspersky experts predict a shift in advanced persistent threat (APT) activity against industrial organisations and OT systems in new industries and locations. The real economy sectors such as agriculture, logistics and transport, the alternative energy sector and the energy sector as a whole, high-tech, pharmaceuticals and medical equipment producers are likely to see more attacks next year. Moreover, traditional targets, such as the military industrial complex, and the government sector will also remain.

Attack surface will also increase due to digitisation in a race for higher efficiency in IIoT and SmartXXX, including systems for predictive maintenance and digital twin technology. This trend is supported by the statistics of attacks on Computerised Maintenance Management Systems (CMMS) in the first half of 2022. In the Middle East, 43,5% of CMMS were attacked in the first half of 2022.

The risks of expanding attack surface are also connected to the rising energy carrier prices and the resulting rises



in hardware prices, would force many enterprises to abandon plans to deploy on premise infrastructure in favor of cloud services from third party vendors and may also affect some IS budgets.

"We saw that cybersecurity incidents were plentiful in 2022 causing many problems for ICS owners and operators. However, we did not see any sudden or catastrophic changes in the overall threat landscape, none that were difficult to handle, despite many colorful headlines in the media. As we analyse incidents of 2022, we must profess that we have entered an era where the most significant changes in the ICS threat landscape are mostly determined by geopolitical trends and the subsequent macroeconomic factors. Cybercriminals are naturally cosmopolitan; however, they do pay close attention to political and economic trends as they chase easy profits and ensure their personal safety. We hope that our

CUSTOMER-FIRST

ANITA JOSEPH, EDITOR, CAUGHT UP WITH **JEAN-GUILLAUME (JG) PONS**, SENIOR VICE-PRESIDENT OF DELL CLIENT SOLUTIONS GROUP (CSG), EMEA, TO DISCUSS HOW THE COMPANY PUTS THE CUSTOMER AT THE HEART OF ALL ITS OPERATIONS.

What's your take on the changing work scenario?

Digital Transformation

and workforce transformation were already underway before the pandemic. All customer conversations were focused on how to perform better from a workforce transformation point of view, when COVID hit. From then on, everything sped up and things that would normally take years, got done fast. The market grew significantly, and everyone wished to accelerate their digital transformation goals since work became remote/hybrid.

We're now in that phase where we see a lot of growth in the market. Transformation is still underway, and companies have completely accepted the need to digitalise their workforce. The conversation between

customers and/or partners are centered around how to enable organisations to be more flexible in the long term, how to integrate hybrid work into the whole organisational and operational structure, IT & digitisation strategy, how to ensure security, help employees be more productive and at the same time, increase their satisfaction levels. Another important question is how to attract and retain talent and provide the right tools to drive employee experience.

Ultimately, work culture is all about productivity and outcomes. So how is Dell's client solutions portfolio evolving to keep up with this whole trend?

What's interesting is that we did not change our strategy. Our strategy is working and we're continuing to work on that strategy. There are three key aspects here: One, we got the end user

at the center of everything we do- from a product innovation standpoint, or even from a product evolution standpoint.

Customers are of different kinds: we've got customers who do field work, others who develop applications, customers who are on the go and travelling all the time, and so on. So, keeping the customer at the center is something we've been doing and continue to do. We also carry out plenty of surveys and make sure we reach out to and interact with our customers. We then use all these insights to chart our roadmaps and our deployment. So, the customer is first and foremost.

The second one is around collaboration, which was always important but became even more so post the pandemic. The question here is: how do you drive a full ecosystem ensuring collaboration and productivity? And it's not just devices, which are of course, important, but also

**OUR STRATEGY IS
WORKING AND WE'RE
CONTINUING TO WORK ON
THAT STRATEGY.**





about the ecosystem around the device—how you integrate everything and ensure seamless collaboration. This is another key focus area for us.

Thirdly, we shifted our innovation piece. For instance, we launched the Dell Optimizer software application that intelligently optimises the performance of systems by using Artificial Intelligence and Machine Learning. It understands a user's behavior when they use the device and helps them be more productive.

Along with remote work, we also see a lot of companies where employees are coming back to the office. So, we're looking at hot desk solutions. How do you interact when you're there? How do you create a seamless experience with docking stations, energy, space and

collaboration? So that's the third area we're focusing on.

How is Dell setting the tone for the hybrid work industry in creating workplaces of the future?

You start from outcomes. You begin with what you want to drive as an organisation to attract talent, retain talent, be productive and drive collaboration. You start from the business outcome or the customer's goals and how we can help them get there. We have a lot of customers we are working with, where we design with them where they want to be, what is the employee experience they want to drive and how to get the required monitoring tools to leverage all of that and drive business outcomes. What's

interesting there is that the conversation is also evolving from casual to serious, where clients are depending on us to help them achieve their business goals.

The Middle East region we know, is evolving and dynamic. What's Dell's plan for this region, particularly given the background of its rapid digital transformation and the growth of hybrid work?

This region is extremely important for us—it's a dynamic one full of opportunities. The economies here are growing fast and the pace of digital transformation is accelerating, particularly in the UAE, Saudi and Egypt. So, we're working with governments and private companies to make their digital transformation journey seamless and smooth. Again, we're looking at this from an end-user point of view which is at the heart of everything we do, and then again, we're leading in most of the areas where we operate in, so yes, this market is huge and very innovation centered. It's an exciting region to be in. 📍

THE CONVERSATION BETWEEN CUSTOMERS AND/OR PARTNERS ARE CENTERED AROUND HOW TO ENABLE ORGANISATIONS TO BE MORE FLEXIBLE IN THE LONG TERM.

Efficient SMB/SME Access & Aggregation Solution

Smart Managed Switches



DGS-1250 Series

The D-Link DGS-1250 Series Smart Managed Switches are the latest generation of switches to provide increased Power over Ethernet (PoE) output, high port density, multiple management interfaces, and advanced Layer 2 features. With all of these features combined, the DGS-1250 Series provides a cost-efficient and flexible solution for expanding any business network.

Power & Value

Deliver real value as an Enterprise Access and Small-to-Medium Business (SMB) Access/Aggregation solution.

Management Versatility

Comes with the D-Link Network Assistant (DNA) utility so admins can remotely control their network to the port level.

D-Link®



RANSOMWARE PRIMARY THREAT TO ORGANISATIONS GLOBALLY: MIMECAST

THREAT ACTORS REFINE ATTACKS TO CAUSE DEVASTATING DAMAGE TO ORGANISATIONS IN MIMECAST'S LATEST STATE OF RANSOMWARE READINESS REPORT

Mimecast, an email and collaboration security company, has released its latest State of Ransomware Readiness 2 report, revealing that ransomware has become a primary threat to organisations worldwide, with Middle Eastern companies not spared from the devastating impact of ransomware attacks.

The report found that 59% of cybersecurity leaders in the UAE have seen the number of cybersecurity attacks increase or stay the same over the past year, with 39% saying they've experienced significant downtime due to a ransomware attack.

Mimecast's State of Ransomware Readiness 2 report is based on insights from 1100 cybersecurity decision-makers in Australia, France, Canada, Germany, the Netherlands, the Nordics, Singapore, South Africa, the UAE, UK and US.

THE RESEARCH FOUND THAT 94% OF GLOBAL CYBERSECURITY LEADERS BELIEVE MORE BUDGET IS REQUIRED TO COMBAT RANSOMWARE.

According to Werno Gevers, cybersecurity expert at Mimecast, business and security leaders see ransomware attacks as virtually inevitable. "Seventy-five percent of businesses in the UAE reported they experienced a ransomware attack in the past year, ahead of a global average of 64%. The consequences can be devastating: a third of UAE cybersecurity teams have experienced an increase in the number of absences due to burnout following an attack, while 23% have seen changes in the C-suite due to a successful ransomware attack."

The report further found that 44% of UAE organisations have experienced a

loss in revenue due to a ransomware attack in the past twelve months. This may partly explain why nearly half (46%) of cybersecurity professionals in the UAE are considering leaving their role in the next two years due to stress or burnout, with 73% of cybersecurity leaders in the region saying their role gets more stressful every year.

Gevers says the research also found that 94% of global cybersecurity leaders believe more budget is required to combat ransomware, with 24% of UAE organisations seeking an increase of 11% to 20% in their annual cybersecurity budgets.

"Cybersecurity leaders need to focus on proactively reducing the chances of a ransomware attack causing disruption. Organisations need integrated security tools to improve threat detection capabilities and relieve pressure on busy security teams. Good fundamental security practices must be in place to reduce vulnerabilities, and security teams need to evaluate crisis planning to understand the real consequences of an attack. It is also essential that leaders acknowledge that cyber risk is business risk, and not leave the financial and personnel resource burden to only IT teams."



MAKING COMMUNICATION SIMPLE

JS WONG, CEO AT SENDQUICK ON THE IT TRENDS DRIVING THE BUSINESS LANDSCAPE AND THE COMPANY'S PLANS FOR THE REGION.



Can you tell our readers about some of the solutions and partnerships that were in focus during GITEX this year?

We are based in Singapore, but we have been working in the Middle East for the last couple of years and we have been focused on mastering our solutions, particularly sending messages to your mobile phones.

We offer on-premises, cloud, hosted service, and even virtual machine deployment options for our mobile messaging solutions. This enables us to tailor our enterprise mobility solutions to your unique company requirements.



The channels of internal and external communication are greatly simplified by our strong SMS gateway and corporate mobility services, enabling your business to immediately address the concerns of all stakeholders.

In the last 12 months, how has your company performed in the MENA market?

The last months were difficult as everyone was still recovering from the pandemic, but we are happy to see the excitement and vibrancy happening again in Dubai, so in the next year we look forward to more developments and sales in all the GCC countries.

Which technologies and IT trends are the forefront of driving innovation for your business?

There are many areas of technology that can be used in our business, such as AI, and we provide dependable enterprise mobility management services to help you keep on top of issues and enhance communications across the entire business.

Better communication speed up problem solving. Employees may cooperate and interact with their co-workers, suppliers, and clients in real time thanks to our mobile messaging solutions and SMS gateway.

Can you tell our readers how your business model has driven key business outcomes for your customers - and what differentiates your company from your market rivals?

We have a couple of business models in our organisation and systems solutions to fulfil all the requirements of our customers. We are very focused in the IT notification space, where there are very few failures and it's very comprehensive. We offer compatibility with all the systems, provide the features that all IT managers require for operations and all types of messaging formats. 🗝



CYBER EXTORTION & RANSOMWARE TOP GLOBAL THREATS: REPORT

SECURITY NAVIGATOR 2023, THE ANNUAL SECURITY RESEARCH REPORT BY ORANGE CYBERDEFENSE, SHEDS LIGHT ON THE CYBER BATTLES BEING WON AND LOST.

Orange Cyberdefense, the specialist arm of Orange Group dedicated to cybersecurity, released its annual security research report, the Security Navigator 2023. Amongst other things, this year's in-depth analysis examined 99,506 potential incidents that were investigated

and triaged by our CyberSOC teams, an increase of 5% from the 2022 report. While this year's report shows encouraging signs that the pace of incidents is slowing, several factors are still a cause for global concern.

This year's report suggests that cyberbattles are being won in some areas. However, many challenges remain.

Cyber-extortion remains the dominant form of attack but victim location is clearly shifting from North America towards Europe, Asia and emerging markets

Ransomware and cyber extortion attacks continue to prove a major threat to organisations globally, and as such featured regularly in Orange



IT VULNERABILITIES IN MANUFACTURING TOOK AN AVERAGE OF 235 DAYS TO BE PATCHED VERSUS AN AVERAGE 215 DAYS ACROSS ALL OTHER SECTORS.

For most industries the majority of incidents we detect are triggered internally, but for our clients in healthcare we attributed an astonishing 76% of incidents to external actors like criminal hackers and APTs (state-backed threat actor groups).

The manufacturing sector remains the number one industry in terms of for cyber extortion (Cy-X) victim count, though our research shows it to rank only 5th amongst industries most willing to pay ransoms. We report that criminals are compromising 'conventional' IT systems, rather than the more specialised Operational Technology, and attribute this high number of victims primarily to poor IT vulnerability management. Indeed, our data shows that businesses in this sector take an average of 232 days to patch reported vulnerabilities. On this metric, only four other industries ranked worse than manufacturing.

IT vulnerabilities in manufacturing took an average of 235 days to be patched versus an average 215 days across all other sectors. In hospitals (within the healthcare and social assistance sectors), IT vulnerabilities took an

average of 491 days to patch. In the transportation sector, patches took an average 473 days.

The average time taken by our ethical hackers to discover a confirmed Serious (High or Critical) Finding was 7.7 days.

The report enumerates how higher levels of security monitoring improve the efficacy of controls, but also generate more false positives and may result in more strain on security professionals. This in an industry struggling to fill over 300,000 cybersecurity job vacancies in EMEA alone.

Mobile security: iOS vs Android

For the first time, Security Navigator 2023 includes proprietary data on the patch levels of almost 5 million mobile devices that it interacted with between September 2021 and September 2022. Third party research suggests that in 2021 both iOS and Android dealt with their fair share of vulnerabilities with 547 vulnerabilities reported for Android and 357 for iOS. 79% of Android Vulnerabilities were considered to have a low attack complexity (trivial for actors to exploit) compared with just 24% for

Cyberdefense's World Watch threat advisories throughout the year. Notable spikes in news about ransomware occurred in March and April, resulting from Lapsus\$ activity and Conti leak events, as well as concerns about the war on Ukraine.

Simultaneously, 40% of the incidents processed by our CyberSOCs involved malware.

Small-to-medium sized businesses are especially forced to deal with malware incidents, reflected in the 49% of confirmed incidents for this group this year (compared to 10% in 2019, 24% in 2020 and 35% in 2021). With average data breach costs estimated at \$1.9 million for businesses with less than 500 employees, SMEs may face the risk of going under due to these breaches.





iOS. 45 iOS vulnerabilities received a critical CVSS score compared to just 18 on Android.

The Navigator report examines serious vulnerabilities in both Apple and Android to determine how long it takes the ecosystem to deploy the required patch. In one iOS case we determine that it took 224 days for 90% of the Apple ecosystem to upgrade to the patched version. For both Android and iOS it appears that about 10% of the user base will never be properly patched.

Findings show that a higher proportion of iPhone users are at risk of being

OUR ETHICAL HACKING TEAMS REPORT A 'SERIOUS' (CRITICAL OR HIGH) ISSUE IN ALMOST 50% OF ALL THE TESTS THEY CONDUCT.

vulnerable when a security issue is first disclosed, due to the homogeneous nature of the ecosystem. Users migrate to a new version quickly, however, with 70% updating within 51 days of the patch being released. The more fractured nature of the Android ecosystem means that devices are often left vulnerable to more old exploits, while fewer may be vulnerable to new exploits.

"The last few months were particularly dense in terms of macroenvironmental events, nevertheless the cybersecurity ecosystem emerges more vigilant and united as a result. Cyberattacks are making headlines, and the war in Ukraine is a resounding reminder that our digitised world is also the field of virtual

battles," said Hugues Foulon, CEO, Orange Cyberdefense.

"The encouraging overall slowdown in the number of incidents for our most mature customers (+5% compared to +13% the previous year) shows that we are able to win battles against malicious actors. However, these successes should not slow down our efforts in the fight against cybercrime. This year's results highlight the challenges faced by organisations of all sizes. Threats are evolving, becoming more complex, coming from all directions and underlining the importance of the work we will continue to do to adapt to the threat and support our customers in this fight," he added. 🔒

**SMES,
MANUFACTURING
AND PUBLIC SECTOR
ARE PARTICULARLY
VULNERABLE.**

Today's IT agility is built on observability.

SolarWinds® Hybrid Cloud Observability helps ensure services and online applications are available, operate cost effectively, and deliver a fantastic and predictable digital experience.

- » Modernize IT agility
- » Accelerate cost savings and time to value
- » Resolve issues faster with deep visibility and context
- » Improve user experience and service availability
- » Value across IT Ops, Dev Ops, and security



Learn more about Hybrid Cloud Observability and how we're re-envisioning the solutions you need to drive business results.

Visit solarwinds.com to learn more.

NEXT-GEN CYBER DEFENCE

I **NED BALTAGI**, MANAGING DIRECTOR – MIDDLE EAST AND AFRICA AT SANS INSTITUTE, TELLS ANITA JOSEPH, EDITOR, SECURITY ADVISOR MIDDLE EAST, THAT AS MORE AND MORE SKILLED WORKERS BECOME KEY TO DEFENDING MODERN ORGANISATIONS, THERE IS A RISE IN DEMAND FOR EQUIPPING PEOPLE WITH THE RIGHT KIND OF SKILL(S).

W **hat's the threat-security landscape looking like, particularly post the pandemic, and how equipped are businesses in the region to deal with this?**

In the field of cybersecurity, there are always new vulnerabilities, threats, and attacks. Organisations must make sure that their workforce is informed and equipped to defend against these ever-evolving threats. To manage these risks, professionals in the field must constantly learn new skills, develop existing talents, and strengthen their expertise.

Following the pandemic, the cyber threat landscape in the Middle East is continually evolving, especially considering the emergence of hybrid workplaces and the growing adoption of technology to increase efficiency and performance in the workplace. Increasingly, attackers are targeting remote workers with more sophisticated spear phishing attacks. We are also seeing significant trends in attacks against remote

access infrastructures, including remote desktop environments, VPNs, and especially improperly configured cloud infrastructures. Furthermore, supply chain attacks and inserting malware by undermining Continuous Integration / Continuous Delivery (CI/CD) software development pipelines are a major concern. Businesses must take action to safeguard their data, infrastructure, and personnel by regularly educating their cybersecurity specialists to remain vigilant, detect threats, and thwart cyberattacks.

We all know there is a critical shortage of skills in the cybersecurity field. But how bad is it, particularly in the region?

Cybersecurity will always be relevant for as long as data, assets, infrastructure, and digital systems exist – they will always require protection from external



**CYBERSECURITY WILL ALWAYS BE
RELEVANT FOR AS LONG AS DATA,
ASSETS, INFRASTRUCTURE, AND
DIGITAL SYSTEMS EXIST – THEY WILL
ALWAYS REQUIRE PROTECTION FROM
EXTERNAL ATTACKS.**



attacks. We can see an active and growing interest in cybersecurity and addressing the shortage within the region, so there's that assurance that the gap is not being ignored as more organisations are investing in training resources and both employees as well as employers are willing to bridge it by the day. We are seeing a particular need for staff that is well trained in defending cloud infrastructures, devising robust secure architectures for enterprise defense, conducting detailed digital forensics and incident response, and performing more complex penetration tests to find and eliminate flaws. Additionally, as more skilled workers are required to defend modern organisations, demand is rapidly increasing to prepare people who are new to cyber to support their organisations' cyber defense. Organisations are not only

looking to upskill their current employees, they are also looking to build the next generation of cyber defenders.

All types of talents are in high demand and there are a wide variety of opportunities in the cybersecurity sector, both worldwide and regionally in the

SANS COURSES ARE NOT JUST LIMITED TO CURRENT CYBERSECURITY PROFESSIONALS, OR HIGHLY EXPERIENCED AND SENIOR CYBERSECURITY PROFESSIONALS.

GCC. Currently, there is a growing need for trained and certified professionals, particularly as businesses look to upskill their workforces and take proactive measures to protect their operations. Additionally, there has been a significant increase in the number of people in the Middle East, particularly in the UAE and Saudi Arabia, who want to learn about cybersecurity.

Why do you think there is so much skill shortage in the field? What's holding people back?

One of the main reasons for the disparity is that people are often intimidated by cybersecurity and technology in general, believing it is too "unfamiliar", "complex" or "technical". Cybersecurity is actually very simple once understood and it's important for organisations to break



those stigmas and make it accessible and approachable. Gamification and building skills through hands-on labs and exercises are immensely helpful tools in this process.

The first step in doing this is by incorporating foundational cybersecurity awareness and training programs into general training. Organisations should also invest in retraining and upskilling their existing senior staff to ensure that all departments are equipped, and not just IT teams. It's vital to ensure such efforts are focused on modern technology stacks, and not on the infrastructures of 10 or 20 years ago. Organisations should look for training that addresses multi-cloud infrastructures, remote worker environments, multi-factor authentication, identity and access management, and more. In addition to strengthening an organisation's

ULTIMATELY, THE MORE PEOPLE THAT ARE AWARE, CAPABLE AND PROACTIVE, THE BETTER PROTECTED THE REGION WILL BE.

overall safety, training all staff members on security awareness and teaching them the fundamental techniques cybercriminals use will not only improve the overall security of the company but also guarantees that the entire workforce is confident, knowledgeable, and proactive in dealing with digital threats.

In light of the talent shortage in the Middle East, how is SANS working to close the cybersecurity skills gap?

To upskill regional cybersecurity practitioners, we organise as many

training events as we can for the region each year, including SANS Gulf Region in Dubai last month, and SANS Summer Dunes in Saudi Arabia. In building these events, we are focused on providing courses in the specific technology areas most in demand, with practical hands-on training that attendees can apply the very next day they get to the office. Where possible, our expert instructors are present to offer in-person support, or we conduct virtual Live Online sessions for students. We also make sure there are active opportunities for participants

following the event that will keep them engaged and allow them to put what they have learned into practice right away.

In addition to our core training solutions and certifications, we offer assessments and programs that help employers uncover existing talent within their organisations. Finding the right talent to fill these roles can be difficult for firms due to the lack of skilled workers in the market. By retraining and upskilling current employees, our Cyber Immersion Academies help firms identify internal cybersecurity talent inside their workforce. We also assist governments by establishing specialised programs to identify and train individuals who are unaware of their aptitude for cybersecurity.

SANS courses are open to career changers, online self-driven learners seeking new skills, college and university students, business professionals without a strong cybersecurity background, new hires in IT/cybersecurity, and participants in reskilling programs. They are not just limited to current cybersecurity professionals, or highly experienced and senior cybersecurity professionals. Ultimately, the more people that are aware, capable and proactive, the better protected the region will be.

We have several ways of helping non-technical professionals break into the cybersecurity industry as well. This includes our beginner-focused paid programs like CyberStart and SANS

ORGANISATIONS SHOULD INVEST IN RETRAINING AND UPSKILLING THEIR EXISTING SENIOR STAFF TO ENSURE THAT ALL DEPARTMENTS ARE EQUIPPED, AND NOT JUST IT TEAMS.

Foundations, but we also offer a wealth of free materials and online resources to the cybersecurity community which all aim to improve their skills and prospects of entering the industry.

For those wishing to launch a career in cybersecurity, we designed the SANS Foundations course. SANS Foundations offers fundamental IT and computer skills that are integral for future careers in the field.

CyberStart was primarily created to engage and excite aspiring youngsters between 10 to 18 years old about a rewarding career in cybersecurity. It offers cybersecurity training through a fun, gamified approach. We found that adolescents are hardly aware of the career opportunities in cybersecurity. Stereotypes like "cybersecurity is just for boys" or "they need to know math or code" are frequently to blame. CyberStart is an excellent method to overcome these biases because cybersecurity is for everyone, regardless of gender or age.

The platform has different storylines and enables users to take on various tasks while learning more about cybersecurity as they play. It was developed to help young students find their hidden talents and expand their knowledge and abilities, and so far, it has assisted hundreds of thousands of students in discovering their potential in cybersecurity.

Adults can also enroll in CyberStart to learn more about cybersecurity and to educate themselves in a fun and interactive easy-going method on the necessary skills to lay the groundwork for a future in the field. Whilst the program itself is subscription based, we also offer governments the possibility of collaborating and setting up extra-curricular activities that integrate with CyberStart.

Today, it's not only important to hire talent, but also retain it. How do you think this can be achieved?

An organisation must make sure that its working conditions are the best in the sector if it wants to keep talent, and this extends to IT and security awareness,

WE HAVE SEVERAL WAYS OF HELPING NON-TECHNICAL PROFESSIONALS BREAK INTO THE CYBERSECURITY INDUSTRY AS WELL.

too. Each organisation should map job roles to the skills required for success in those roles and identify a standard set of training opportunities for those skills. Then, provide employees with the chance to increase their cyber-related knowledge and abilities with organised training courses as well as continuous learning and practice using cyber ranges and other resources. Also,



it is important to make sure there are opportunities to connect and interact with the local cybersecurity community so that their knowledge is up-to-date and relevant to the immediate cyber landscape in the region. They can do this at meetups, trade shows, and online, as well as in Capture the Flag competitions, hackathons, and training seminars like those offered by SANS. This creates

a standard training and certification roadmap that both new and senior-level employees can follow throughout their career development, ensuring their interest is consistently supported.

What can we look forward to from SANS, in 2023?

Next to the various events we are organising across the GCC, SANS is also

introducing various new products that will help organisations better prepare for real-life situations such as data breaches or cyber-attacks. We're in the process of introducing several new courses on vital topics, as well as our process of constant revising and updating our entire line of courses. We're very excited at what 2023 will bring in terms of new courses, new certifications, and new resources. 🗝

SWIMLANE & NOZOMI NETWORKS AUTOMATE SECURITY ORCHESTRATION, THREAT DETECTION & RESPONSE FOR CRITICAL INFRASTRUCTURE



Swimlane, the low-code security automation company, and Nozomi Networks, the leader in OT and IoT security, have announced a technology integration that combines low-code security automation with operational technology (OT) and Internet of Things (IoT) security. The combined solution makes it possible for industrial and critical infrastructure security operations to maintain continuous asset compliance and mitigate the risks of attacks from combined OT and IT entry points.

Critical infrastructure environments such as healthcare, utilities, transportation and food production are increasingly seen as vulnerable and lucrative targets based on the ability to disrupt society. As attacks on critical infrastructure continue to rise, the need to enhance protection for OT and cyber-physical systems (CPS)

with more advanced, low-code security orchestration, automation and response (SOAR) capabilities that cross IT and OT is paramount. Yet, according to Gartner, roughly 90% of OT security teams are still in the remedial phases of protection (e.g. discovery, patching, and firefighting).

"Critical infrastructure is facing a surge in targeted attacks and an ongoing shortage of cybersecurity expertise to detect and respond to these OT and IT attacks," said Chet Namboodri, Senior Vice President of Business Development and Alliances at Nozomi Networks. "By partnering with Swimlane, we are empowering customers with an IT/OT converged and more automated approach to accelerating their response to incidents against their critical infrastructure."

The Swimlane and Nozomi Networks integration elevates the protection of OT and critical infrastructure with multiple benefits:

1. **Real-Time Incident Response**

Capabilities: The integration enables security analysts to respond to threats in near real-time through either a fully-automated response, or via a single-click triage action when human-in-the-loop interaction is required. Presenting OT security operation teams with early detection information helps reduce the risk of the most sophisticated breaches while compressing the mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).

2. **Automated Asset Management, Compliance and Defense**

By leveraging Nozomi Networks robust discovery and vulnerability detection, a complete and autonomous process can be deployed utilising Swimlane to orchestrate managed patching of critical systems, preventative patching across OT assets and a reduced attack surface for would-be attackers.

3. **SOC Automation Suite and System of Record**

The Swimlane platform enables IT and OT security teams to connect their processes through a common lens. This not only provides increased visibility across joint initiatives but enables distributed security personnel to seamlessly work cases as situations dictate using the same interface. 📌

CRITICAL INFRASTRUCTURE ENVIRONMENTS SUCH AS HEALTHCARE, UTILITIES, TRANSPORTATION AND FOOD PRODUCTION ARE INCREASINGLY SEEN AS VULNERABLE AND LUCRATIVE TARGETS.

Secure Your **Digital Future**

Simple. Secure. Resilient.



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

www.raqmiyat.com

UAE | KSA | INDIA



PREDICTIONS 2023

It's been a roller-coaster ride for the cybersecurity industry in 2022. While there were many hits and misses, what has emerged clearly is the need to buckle up our defences and ramp up our security infrastructure, if we are to successfully navigate the uncertainties of the future. The statistics prove it: According to The 2022 Ponemon Institute State of Cybersecurity and Third-Party Remote Access Risk Report, 54% of organisations experienced a cyberattack in the last 12 months, while 75% of

respondents said they've experienced a significant increase in security incidents — most often due to credential theft, ransomware, DDoS, and lost or stolen devices. Clearly, we have lots of work to do to make enterprise environments — both remote and brick and mortar — more secure.

In this context, Anita Joseph, Editor, Security Advisor & Tahawultech.com, caught up with some of the leading lights of the cybersecurity industry to find out what they think 2023 holds. Here's what they said.

WIPERWARE TO CONTINUE DESTRUCTIVE RUN:BARRACUDA

■ FLEMING SHI, CTO

Russia's invasion of Ukraine this year revealed the modern digital battlefield. Most notably, we have witnessed an increased use of wiperware, a form of destructive malware against Ukrainian organisations and critical infrastructure. The frequency has dramatically increased as we saw WhisperGate, Caddy Wiper, HermeticWiper, and others hitting the news since the war broke out. Unlike the financial motivations and decryption potential of ransomware, wiperware is typically deployed by nation-state actors with the sole intent to damage and destroy an adversary's systems beyond recovery. In addition, in 2023, wiperware emanating from Russia will likely spill over into other countries as geopolitical tensions continue; and hacktivism by non-state actors seeking additional measures to exploit victims. To ensure business continuity despite an attack, it's imperative for organisations to focus on full-system recovery that provides operability of the entire system instead of just data. For example, a speedy restoration of the virtual version of a targeted physical system will



WIPERWARE STEMMING FROM GEO-POLITICAL TENSIONS WILL SPILL INTO OTHER COUNTRIES.

dramatically improve the resiliency of your business against wiperware or other destructive malware attacks.

Ransomware gangs will become smaller and smarter

Throughout 2022, the major ransomware gangs—LockBit,

Conti, and Lapus\$—were behind blockbuster attacks, keeping them in the headlines. But in 2023, with the ransomware-as-a-service business model taking off and the recent build leak of LockBit 3.0, a new generation of smaller and smarter gangs will steal their limelight. During the year, organisations will experience an increased frequency of ransomware attacks with new tactics, and those that aren't prepared will make headlines that devastate their business and reputation. 🔑

CYBER HYGIENE & AWARENESS TO BE TOP PRIORITY: DELINEA

■ JOSEPH CARSON, CHIEF SECURITY SCIENTIST & ADVISORY CISO

The digital world is evolving quickly with AI (Artificial Intelligence) and quantum computing expected to soon become a reality. When it comes to cybersecurity, we must always try to determine where we need to be and how to align our security strategy to that possible future. With ransomware continuing to adapt with different enhancements and tactics, we must always be dynamic and flexible to change. Attackers are always evolving and looking for ways to gain access.

Yet, while some things change others stay constant. Data privacy and security continue to be a top priority and as the working environment our homes have become an extension of the office. And cloud continues to be an increasingly massive expansion of the threatscape.

Deep Fakes Replicate Digital Humans – The Digital DNA Theft

In 2023, Deep Fakes will become so authentic that not only will we see our digital identities being stolen, but also digital versions of our DNA. Exposing our Digital DNA on the internet will enable Deep Fakes to replicate and create Digital Humans.

If you have ever seen the movie “The 6th Day,” we are on the same path for replicas of our digital selves. Humans sync our physical lives on social media with constant uploads of photos, videos, audio and personal preferences with enough data points and some enhanced algorithms.

It is only a matter of time before attackers can create lifelike digital avatars of anyone, and it will be incredibly difficult to identify the difference without technology to analyse the source data.

Bring Your Own Office (BYOO)

Employees’ homes will become extensions

of company offices. Just as Cloud Transformation dominated the pandemic period, we have now started the Bring Your Own Office transformation, where employees’ home networks have become cloud droplets or mini clouds.

The big challenge for organisations today is knowing where the organisation’s security start and stop, and should they be attempting to secure employee homes as an extension of the corporate office.

And what would that mean for the employees’ data privacy? Do we all become always-on employees where we are no longer an employee nine to five?

In the past your personal life and corporate life had a clear separation. With Bring Your Own Device that dynamic changed, and now with Bring Your Own Office it will continue to evolve even further. The boundaries will become even blurrier.

The Cyber Basics – Cyber Hygiene and Awareness

The need to become a cybersecurity society will see an increase in getting the basics right. This means that cyber hygiene and awareness will be a top priority in 2023.

With more organisations looking to obtain cyber insurance as a financial safety net to protect their businesses from serious financial exposure resulting from data breaches and ransomware attacks, the need to get a solid cyber strategy in place will be mandated to get insurance. The days of “cheap and easy” are over.

This means getting back to the basics in 2023 to level up cybersecurity baselines. Ongoing remote work and cloud transformation means that a strong access management strategy will be needed supported by multifactor authentication, password management and continuous verification to reduce the risks.

In addition to implementing better access security controls, employers will



need to empower workers with better cybersecurity awareness. This means ongoing training and education to ensure that as threats evolve, employees are informed and ready to be strong defenders in cyber strategies.

Cyber Armies – The Offensive Gets Real

Over the past few years, we have seen many countries explore capabilities to go on the cyber offensive. As a result, this will see the introduction of cyber armies.

Many countries have already adopted some variation of a cyber force, whether to support existing armed forces or to defend the country when targeted by cyberattacks, such as what Estonia did as a result of the 2007 cyber-attack. In 2010 Estonia established the Estonian Defence League Cyber Unit which continues to prepare and simulate when a cyberattack targets the country so they are ready to defend the country.

Many other countries have since also established similar units. Now the need to get offensive has now become a reality.

The reality is that while many countries may not have traditional weapons, all countries can easily build cyber weapons – and be ready to use them.

The Cyber Workforce Quest

Each year the cyber talent gap is increasing. As an industry we must accelerate how to get more new talent and diversity to join the cybersecurity workforce. 🔑



SILOED SECURITY TECHNOLOGIES WILL BECOME WEAKEST LINK: LOOKOUT

■ SUNDARAM LAKSHMANAN, CTO

Specialised point products will become the Achilles' heel of enterprise security. Put aside the problems or the breaches of the future for a moment. Even the current breaches we are seeing now cannot be prevented or responded to or remediated unless organisations start thinking about cloud-delivered, integrated security platforms. Without this, the problem will be harder and harder for companies using siloed point products— regardless of whether they're

hosted on-premises or in the cloud.

The warning signs are everywhere: data security best practices sometimes fall through the cracks and breaches are becoming incredibly complex. As data, devices, and users continue to become more interconnected, IT and security teams need to consolidate their security solutions to avoid the complexities of trying to secure data with multiple tools. The platform approach will help ensure that all data— regardless of whether it lives in the cloud, on-prem, or in a private app — is being protected under

uniform data security policies.

For the next few years, this issue should be top-of-mind: there is simply no other way for enterprises to easily stop breaches or troubleshoot a breach or respond to a breach or understand the breach without the visibility and control that a platform approach can provide.

The secure services edge (SSE) market is proving that a combination of cloud access security broker (CASB), zero-trust network access (ZTNA), and secure web gateway (SWG) in a single platform is the most forward-looking approach to securing remote workers and protecting data across the modern enterprise infrastructure. A recent survey by Gartner, Inc. found that 75% of organisations are pursuing security vendor consolidation in 2022, up from 29% in 2020. ■

→ **THE PLATFORM APPROACH WILL HELP ENSURE THAT ALL DATA— REGARDLESS OF WHERE IT LIVES— IS BEING PROTECTED UNDER UNIFORM DATA SECURITY POLICIES.**

OT SECURITY IN 2023: TIME TO SHOW THE RECEIPTS

DANIELLE JABLANSKI, OT CYBERSECURITY STRATEGIST, NOZOMI NETWORKS

There has been broad realisation in the public that operations which tolerate little to no physical downtime – including critical infrastructure, industrial sectors and hyperconnected facilities – are lucrative targets for cyber-attacks. A decade ago, intrusion and anomaly detection tools for operational technology (OT) and industrial control systems (ICS) were in their infancy. Today, the market is expanding and maturing in new ways.

Despite IT and OT being substantially different fields with divergent priorities, several cybersecurity companies traditionally serving IT have already entered the OT cybersecurity market. With market analysis predicting a major boom, leaders in the market will find themselves at a more crowded table in 2023. Detection, digital transformation, operational reliability, interoperability, governance and standards continue to drive demand.

If any theme has emerged from 2022 it is that trust and verification for OT cybersecurity are not mutually exclusive.

Zero Trust has taken on a life of its own with a myriad of definitions and implementation mechanisms from strategy to application. With an assume breach mentality, recognizing that perimeter security is insufficient to defend against today's threat landscape, Zero Trust principles are essential to reduce "dwell time" and the severity of potential impacts.

Some may say Zero Trust is simply repackaging best practices like network segmentation and the principle of least privilege, but properly applying Zero Trust requires studying how technologies interact, what they need from each other, and how to minimize superfluous access to information, command, and control of systems.

What's on the horizon for 2023?

From the now-or-never razzmatazz surrounding SBOMs (Software Bill of Materials) to the next unprecedented international issue, predictions are difficult to master. Predictions are even more difficult for OT and ICS given that data is often either private, distributed, or behind a paywall. 2023 promises to be an integral year, calling for increased cybersecurity investments at a time when a potential recession can exacerbate the impacts of ransomware and unplanned downtime or production loss.

Governance will set new precedence

Government standards and frameworks to date have taken an accordion approach, stretching to address what critical infrastructure sectors have in common, and compressing to magnify security issues most critical to specific sectors. New direction and bolstered industry involvement will produce greater situational awareness, trust, and resolve across the critical infrastructure security community. The U.S. government is "putting its money where its mouth is," rolling out a federal binding operational directive focused on asset discovery and vulnerability enumeration, offering implementation assistance and unique tool sets. In addition to the CIRCIA legislation, 2023 will usher in the fruits of two recently debuted CISA programs. The CyberSentry program will monitor critical infrastructure networks for known threats and indicators of compromise, and the newly released RedEye tool, developed to "parse logs from attack frameworks (e.g. Cobalt Strike) will present complex data in a more digestible format. Both will broaden the aperture for understanding of OT and ICS incidents, further building out mechanisms for enhanced trust and verification.



Innovative analysis will set solutions apart

Innovation in the ability to provide situational awareness, with trust and verification, will lead the OT cybersecurity future. Many organisations enable tools to gather and store data but fail to analyze data to enhance their mission. Simply having and storing reams of data is not particularly useful for any risk mitigation. Solutions built for OT and ICS will continue to fix security gaps and improve security controls.

The Receipts

The Nozomi Networks-sponsored SANS report on the state of ICS/OT Cybersecurity in 2022 and beyond mentions "adversaries in critical infrastructure networks have illustrated knowledge of control system components, industrial protocols, and engineering operations." Other reports of OT/ICS incidents cite adversaries' "unfamiliarity with the OT domain." 2023 may be the year that adversaries demonstrate increased capabilities to both monitor – and modify OT and ICS systems in critical sectors. Across the globe, governments, public-private-partnerships, insurance providers, and international relations are reticent about the significance of protecting critical infrastructure and building resilience across industrial sectors and hyperconnected facilities. Across the market – from competitive intelligence to innovation to live "bake-offs" – trust and verification matter more today for OT cybersecurity than ever before. OT cybersecurity stakeholders, concerned with physical safety, environmental impacts, the provision of goods, services, and resources, micro and macroeconomics, will all be saying "show me the receipts" in 2023. 📄

WHAT'S NEXT?

TAMER ODEH, REGIONAL SALES DIRECTOR, SENTINELONE

As we get better at defending the endpoints, threat actors will need to up their game in order to penetrate harder targets.

2022 was a sobering year for us all. Riding on the back of the COVID pandemic of the previous two years, we entered a new reality with war returning to Europe in a way not seen since 1945. And yet along with tanks, missiles, and the targeting of civilians and civilian infrastructure came a new battlefield: cyber warfare with wipers being used to hit targets inside and outside the physical battleground.

Meanwhile, new attack surfaces came to the fore, as cybercriminals began to understand how to exploit identity for access and cloud workloads for assets, privilege escalation and lateral movement.

It's not been all bad. Evolving security technologies like XDR are helping organizations to fill the gaps in visibility, join the dots in defense, and hunt for hidden threats in the enterprise. Law enforcement at home and abroad has been capturing and incarcerating more cybercriminals than ever before, while also closing the doors on some of the darknet's worst illicit markets.

As we enter 2023, we need to accept that hardware multi-factor authentication, short lived sessions, and severely curtailed account privileges aren't nice-to-have paranoid bells and whistles. They are now the entry threshold of the aspirational standard of corporate security.

Cybersecurity Only Works When "It Just Works"

2022 has been a year where, compared to previous years, the cybersecurity market has adapted not just to the threat landscape but perhaps more strongly to how security teams want to use cybersecurity products. This is something I expect to see much more of in 2023.

Demand for More Vendor Collaboration

As much as we expect consolidation, customers will always end up using more than one vendor. We're already seeing security teams demand more integration and more value from the collaborations between vendors. Gone are the days when a "technological alliance" could mean little more than a shared video. In 2023 this will range from a demand for integration across more types of use-cases and standardisation of data models to a very legitimate expectation that every new vendor will not only provide value on its own but also help extract more value from the existing products in the security stack.

Cost Will Be a Driving Force

The economic turmoil will pressure enterprises and organizations to save on costs and be more effective. As a result, expect more consolidation of pinpoint tools and teams and more utilization of growth and efficacy enablers like moving to the cloud.

Prediction: With less security budget, efficiency-driven products will strive. The cost will become the main consideration for cybersecurity programs.

The Disruptors Are Here, And They Aren't Going Away

2022 has been the year of disruption by non-traditional threat actors. Flaws in how teenagers exploited the way the traditional cybersecurity establishment thinks. Advances in computing power and AI will transform the effectiveness of social engineering, fraud, and active measures (information/influence operations). As governments try to get a handle on asymmetric threats, new ways of attacking the global problem will have to be used.

Deep Fakes Will Enhance Social Engineering

As we get better at defending the endpoints, threat actors will need to up



their game in order to penetrate harder targets. Social engineering remains a popular vector of attack, especially as workforces continue to remain decentralised and remote. Increases in computing power and availability of AI/ML engines will accelerate the effectiveness and authenticity of social engineering attacks through audio and video.

No More Hiding Behind Our Macs

Indicators of what we might expect in 2023 can be read in the tea leaves of our roundup of macOS threats in 2022. The year just ending saw something rare in the macOS threat landscape become common: the inclusion of Mac payloads appearing in numerous cross-platform attack frameworks. While this wasn't entirely unheard of in the past, it was not the norm, and Mac payloads were generally poorly written, unreliable and, frankly, unsuccessful.

What's changed is the increasing popularity of two things: performative and stable cross-platform languages like Go, Kotlin and Rust, and Mac devices in the enterprise. The first makes it easier for threat actors to write Mac-compatible malware, the second gives them the motivation to get better at it.

In 2023, expect to see threat actors target macOS more successfully with cross-platform malware and to expend more effort on finding windows of opportunity to compromise unpatched Macs with known bugs. More supply chain attacks on developers and shared repositories are also likely to feature in 2023. 🔑

HEIGHTENED HACKTIVISM AND GEOPOLITICAL CYBERATTACKS IN 2023: TRELLIX

Trellix, the cybersecurity company delivering the future of extended detection and response (XDR), released its annual threat predictions report for 2023. Forecasts from the Trellix Advanced Research Center anticipate spikes in geopolitically motivated attacks across Asia and Europe, hacktivism fueled by tensions from opposing political parties, and vulnerabilities in core software supply chains.

"Analysing current trends is necessary but being predictive in cybersecurity is vital. While organizations focus on near-term threats, we advise all to look beyond the horizon to ensure a proactive posture," said **John Fokker, Head of Threat Intelligence, Trellix**. "Global political events and the adoption of new technology will breed novel threats from more innovative threat actors."

The Trellix Advanced Research Center brings together hundreds of the world's most skilled security analysts and researchers to serve the global threat intelligence community and organizations with the latest threat indicators and insights collected from Trellix's extensive sensor network.

Trellix Advanced Research Center forecasts the following threats in 2023:

- **Geopolitics and grey-zone conflict.** Geopolitical factors will



Vibin Shaju, VP EMEA, Solutions Engineering, Trellix.

continue to be a high motivation for misinformation campaigns and cyberattacks timed with kinetic military activity.

- **Hacktivism takes center stage.** As groups of loosely organized individuals fueled by propaganda align for a common cause, they will ramp up their use of cyber tools to voice their anger and cause disruption across the globe.
- **Skeletons in the software closet will multiply.** Both threat actors and security researchers will heighten their study of underlying software frameworks and libraries resulting in an increase in breaches related to software supply chain issues.
- **Increasing activity by teen cybercriminals.** Teens and young adults will engage at increasing levels in cybercrime – everything from large-scale attacks on enterprises and governments to low-level crimes that target family, friends, peers, and strangers.
- **Declining accuracy of code-based attribution.** The outsourcing of malware creation and operation, diversification of malware development, and use of leaked source code will make attribution of cyberthreats to specific threat actors increasingly challenging.
- **Imminent global cyberthreat to critical infrastructure as cyberwarfare evolves.** A significant rise in advanced cyberactors causing disruptions to critical infrastructure in vulnerable targets will be observed.
- **With more collaboration comes more phishing.** Weaponized phishing attacks will increase across commonly used business communication services and apps, like Microsoft Teams, Slack, and others.



John Fokker, Head of Threat Intelligence, Trellix.

- **"Alexa, start mining bitcoins."** The advanced capabilities of consumer and enterprise IoT devices will be leveraged by hackers to mine cryptocurrencies.
- **Space hacking: only going up from here.** The compromise of satellites and other space assets will increase and become more public in 2023.
- **Here's my number, so call me, maybe.** There will be a huge jump in reverse-vishing – or voice phishing – attacks, with less tech-aware users being the primary target.
- **Attacks against Windows domain will scale.** More domain privilege escalation vulnerabilities will be discovered as well as more real-world attacks against Microsoft Windows with the explicit goal of complete network takeover.

"We started 2022 with an industry-wide vulnerability in Log4J, which was closely followed by cyber and physical war targeting Ukraine. We're closing the year observing hacktivists taking matters into their own hands, new actors in operation, and a changed but increasingly active ransomware landscape. As stress continues to weigh on the global economy, as we head into the new year, organisations should expect increased activity from threat actors looking to advance their own agenda – whether for political or financial gain," said **Vibin Shaju, VP EMEA, Solutions Engineering, Trellix**. "To outwit and outpace bad actors and advance defenses proactively, security must be always-on and always learning." 🧑🏻‍💻

SKILLS SHORTAGE TO BECOME TALENT WAR: VECTRA AI

CHRISTIAN BORST AND BRIAN NEUHAUS, CTO, AMERICAS AT VECTRA AI

Supply chain attacks will continue but hackers will look beyond the 'usual suspects' to cause havoc:

Attackers will continue to cause maximum disruption in the form of supply chain attacks, but instead of targeting key suppliers, they will look beyond the 'usual suspects' to gain access into networks. For instance, this could include legal or accounting firms. A holistic approach may help turn the tables on the matter: supply chain means partnership — partnership means collaboration and supporting each other. Only as a 'mesh' interconnected structure with consistent resiliency can companies thrive in the digital economy. This includes ensuring that they review the security policies of all those in the chain.

Increased analyst fatigue and resignation will see the tides turn away from protecting the castle walls to detection and response: Attackers are continuing to breach the castle walls, creating fatigue and eventual resignations amongst cybersecurity professionals. Instead of working on preventing these attacks from happening and to prevent employee burnout, we will see a needed shift to focus on reducing the impact of an attack. This means building resilience within the organisation covering people, process and technology

AMID A GROWING ATTACK SURFACE, THE SKILLS SHORTAGE AND RISE OF UNKNOWN THREATS; ACCURATE AND RAPID SIGNALS WILL BE ESSENTIAL.



Christian Borst



Brian Neuhaus

and focusing on early detection and sound response as opposed to protection & prevention.

Multi-Factor Authentication (MFA) will continue to be a prime target for attackers: With identity attacks on the rise, in 2023 attackers will continue to take advantage of vulnerable MFA methods. As companies continue to roll out MFA, attackers will continue to take advantage, either by flooding end users with requests to brute-force their way in, or by skilled phishing campaigns. End users will be the ones directly targeted by attackers. This means not just organisations, but also consumers will need to be more aware than ever of the risks to their digital identities. Meanwhile, organisations must ensure they have tools in place to detect suspicious login activity and stop it in its tracks.

Attackers will begin to steal and keep encrypted data to decrypt in a post quantum world: Advances in quantum computing will force the hand of security leaders in 2023 to start thinking about this sensitive encrypted data in a post-quantum world. However, this approach will also grab the attention of attackers,

and instead of bypassing encrypted data that was previously safeguarded, they will attempt to grab the data and keep it stored for sale or to be later decrypted.

As the war for talent increases, security companies will need to develop creative ways to recruit and retain workers: As an industry that is no stranger to burnout and stress, cybersecurity companies will have to ensure they can demonstrate they are an attractive outfit to work for. This is in order to fend off competition from tech companies that can often offer lucrative salaries and superior work-life balance. To achieve this, cybersecurity companies must adopt a more forward-thinking approach, this could include offering flexible working arrangements, performance incentives and health and wellness policies.

Software and IOT device labelling take a foothold: Labels should state clear facts about the privacy and information security parameters of the product and organisation. One key piece of information on labels should be how long a company will support its software, because a physical device may outlast the time a product is supported. 📌

Fast. Reliable. Secured
SWITCHING SOLUTION



Save Energy **without**
SACRIFICING PERFORMANCE

DGS-F1210-26PS-E

Layer 2 Gigabit Managed Long Range PoE+ Switch



Highlights

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

D-Link®

Connect to more...

SIMPLIFYING IT

MRIDUL GANGULY, HEAD OF SALES MEA AT ISSQUARED, DISCUSSES HOW THE COMPANY'S KEY OFFERINGS ENABLES CUSTOMERS TO UNDERGO A SEAMLESS DIGITAL AND SECURITY TRANSFORMATION BY BEING ABLE TO SIMPLIFY, DEVELOP, BUILD, AND MANAGE IT SOLUTIONS FOR THEMSELVES.

How has your company performed in the MENA market in the last one year? Has your company ventured into any new markets/countries?

We have expanded our operations significantly in the last couple of years since we started in 2020, in spite of pandemic limiting our growth plans. Though we have 15 offices globally, however from our Middle East & Africa division we have increased our reach by venturing into the African market focussing on key countries like Egypt, Kenya, Tanzania, Uganda, Nigeria, Ghana & even South Africa. We are continuing to explore & partner with key security players in the other market for our niche

products. However, we are confident that with our official distributor we will be able to make faster inroads into the Middle East and African markets. We also focus on creating public awareness about our product lines through social media, email campaigns & webinars and have been quite successful in getting to follow our products.

Which technologies and IT trends are the forefront of driving innovation for your business?

Our key offerings enable our customers to undergo a seamless digital and security transformation by being able to simplify, develop, build, and manage IT solutions for themselves. These products have been carefully designed keeping

in mind the gaps with various product offering & their lengthy implementation cycles. Our automated technologies help customers to leverage on our expertise with our tailor-made solutions to manage digital risk and protect from security breaches across networks, clouds, endpoints, services, users and devices.

Can you tell our readers what differentiates your company from your market rivals?

We believe in keeping things simple and customisable. There are products which have all the functionality within a single module and the customer has to pay for it whether or not it needs it. We have separated these solutions to cater to the key requirements of any customer which





makes it simple, cost effective and easy to implement ensuing a faster ROI for any customer. But if needed these solutions can be well integrated to make it holistic solution to offer a seamless, user-friendly experience which really drives the success of any project implementation.

To give you an example, our ORSUS access manager offers RBA as default, which is uncommon for most of the access management solutions today.

Moreover, typically there are several single solutions under SSO / MFA solution, which need separate license for each. So, OAM gives customer the flexibility & cost saving with single license addressing all functionalities including RBA (Risk based access).

Another example would be, ISSQUARED's OLM & EIAG solution, is a tailor-made solution which is based on the customer needs. It really stands out

because it streamlines the process of managing identities and controlling their access with easy to create workflows without the need of backend scripts, gives the infrastructure flexibility with distributed architecture and help improving operational agility and the overall security posture by periodic & adhoc recertifications. It also value adds further by multiple existing or newly built connectors to any target systems. 📌

A HOLISTIC APPROACH TO ENDPOINT MANAGEMENT

VERONICA MARTIN CAUGHT UP WITH **ROHIT KUMAR**, SALES HEAD AT 42GEARS MOBILITY SYSTEMS TO DISCUSS GITEX 2022 AND THE COMPANY'S PLANS FOR THE REGION.



Can you tell our readers about some of the solutions and partnerships during GITEX this year?

We manage all the endpoint devices which are used by enterprises. We are an industry agnostic product where our product goes into industries such as manufacturing, logistics, education, pharma, automobile and many more.

We have built a unified approach for managing all types of endpoints, apps and content used in a business ecosystem. Our UEM (Unified Endpoint Management) solution empowers IT teams to take a consistent and holistic approach towards endpoint management using a single device. UEM fixes ineffective multi-platform dependencies to provide security and control over all business endpoints.

In the last 12 months, how has your company performed in the MENA market? Has your company ventured into any new markets/countries, and can you share your overall growth?

During the last year we have seen a very good response from the market, as it's now open and the lockdown is over. We have seen a lot of people and companies to show interest to buy our solutions. We expect to grow not less than 50% from the last year in the two upcoming quarters.



Which technologies and IT trends are the forefront of driving innovation for your business?

We are very focused on innovations and keep on changing our products as our customers' requirements. We have a product called CamLock, which can block the camera of the person entering the office.

Our objective is leading the field in cutting-edge enterprise mobility solutions. Along the way, we've been recognised for our unified endpoint management technology, as well as for pioneering cloud solutions for enterprise

WE HAVE BUILT A UNIFIED APPROACH FOR MANAGING ALL TYPES OF ENDPOINTS, APPS AND CONTENT USED IN A BUSINESS ECOSYSTEM.

mobility. We have met every obstacle head-on, and we are eager to see what the future holds for us.

Can you tell our readers and what differentiates your company from your market rivals?

After talking to our customers, we

have realised customers look for good support, service, and flexibility, meaning every customer has different requirements. Some need very specific features, and if we don't have them, we will ensure we will develop them. This is what makes us really stand out from the competition. 🔑

BARRACUDA APPOINTS JOE BILLANTE AS NEW CHIEF FINANCIAL OFFICER

Barracuda Networks, Inc., a trusted partner and leading provider of cloud-first security solutions, has announced Joe Billante as its new Chief Financial Officer. Billante brings more than 20 years of executive leadership and finance experience to Barracuda, and has successfully led companies through business transformations, international expansion, and accelerated growth.

"As we continue to evolve our award-winning security solutions and go-to-market ecosystems, we are excited to have Joe on our team, with his deep expertise in business strategy, financial integrity, stakeholder engagement, and operational excellence, said Hatem Naguib, CEO of Barracuda. "Joe is



a thoughtful decision-maker and innovator, who shares our business vision and commitment to our team."

"I am very proud to join the Barracuda

team and excited for the business opportunities ahead. Barracuda provides customers and partners with the solutions needed to protect their businesses from an increasingly complex security environment," said Joe Billante CFO of Barracuda. "I am thrilled to be part of this important mission and look forward to getting to know and working with our customers, partners, employees and stakeholders."

Billante joins Barracuda most recently from eBay where he spent the last 13 years in several business, finance, and analytics executive leadership roles. Before eBay, he spent 11 years at General Electric in a number of finance roles including CFO for a \$1B international division of GE Healthcare. 📌

GERARD ALLISON JOINS SOPHOS AS SENIOR VP OF SALES FOR EMEA

GERARD HAS A DEEP UNDERSTANDING OF THE DISTRIBUTION AND RESELLER CHANNEL, AS WELL AS EXTENSIVE KNOWLEDGE OF SUCCESSFULLY ESTABLISHING NEW ROUTES TO MARKET.

Sophos, a global leader in innovating and delivering cybersecurity as a service, has announced that Gerard Allison has joined Sophos as Senior Vice President of Sales for Europe, Middle East and Africa (EMEA).

"We are very excited Gerard joined Sophos to lead and help accelerate our growth efforts in EMEA, one of the largest regions for the company. Gerard has a deep understanding of the distribution and reseller channel, as well as extensive knowledge of successfully establishing new routes to market. With this impressive track record, Gerard will be a valuable and important Sophos sales leader overseeing EMEA, particularly as we head into 2023 with our new Sophos Managed Detection and Response service," said Michael Valentine, chief revenue officer at Sophos. "The need for modern cybersecurity solutions, including MDR services from a team of

experts trained to spot intrusions 'hiding in plain sight' along the attack chain, has become imperative, as indicated in the Sophos 2023 Threat Report. Sophos' line up of products, services and threat intelligence capabilities, coupled with Gerard's career expertise in cybersecurity and technology, will ensure our EMEA partners provide customers and prospects with the most advanced security solutions available."

"Sophos is an industry leader, pioneering the way with a new type of MDR service that every organisation can benefit from, so I am thrilled to be joining Sophos at this time and leading the company's impressive sales team in EMEA," said Allison. "I am also looking forward to working closely with our extensive partner network in the region to develop new revenue streams and ensure customers have the proper security needed to defend against today's persistent attackers."

Allison has more than 30 years of



industry experience and is known for his entrepreneurial style and vision, increasing revenue, developing sales programs, training and enablement, building customer and partner engagement, and much more. Allison joins Sophos from Exclusive Networks. He also previously worked at Gigamon and Juniper Networks. He is based in Essex, U.K. 📌

Fortinet Security Fabric

Broad

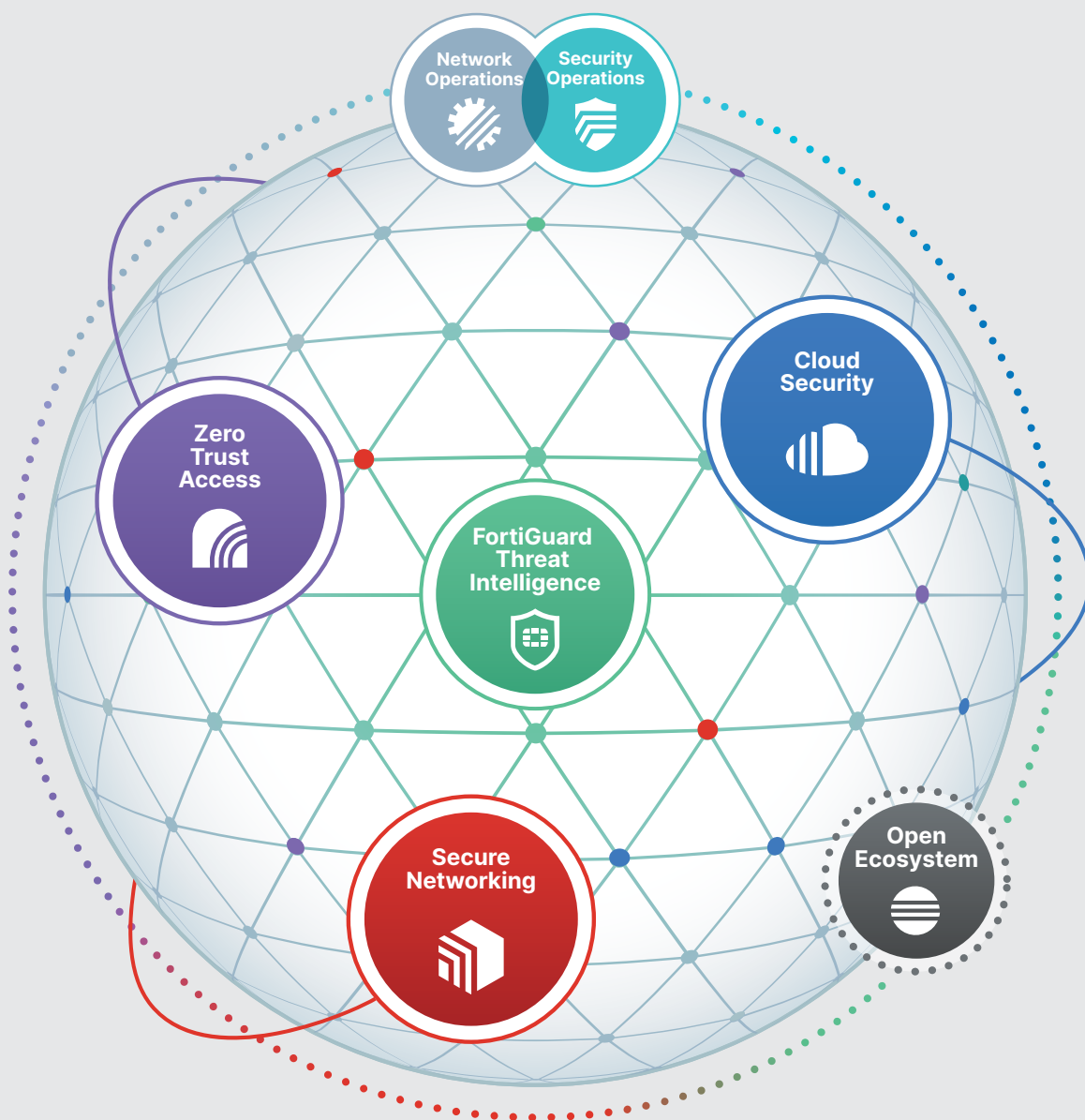
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

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





GROUP-IB ANALYSTS HAVE GONE TO GREAT LENGTHS TO PROTECT THE REGION THROUGH THE DISCOVERY OF A RANGE OF THREATS AT THE HANDS OF MALICIOUS ACTORS.

INTELLIGENCE-DRIVEN SECURITY

ASHRAF KOHEIL, REGIONAL SALES DIRECTOR, MEA HQ AT GROUP-IB, TELLS ANITA JOSEPH THAT EDUCATION AND AWARENESS OF THE END USER IS KEY TO SECURITY, AS ONE WRONG CLICK CAN DESTROY A BUSINESS COMPLETELY.

In the rapidly changing cybersecurity ecosystem, how does Group-IB position itself?

At Group-IB, we believe that cybersecurity is all about having a full ecosystem. This ecosystem needs to be complementary and agile. Complementary means not replacing anything that the clients currently have in terms of technology—it's all about moving your environment from good to great or great to excellent.

The second key factor is knowledge transfer. What's unique about Group-IB is that culturally, inside the organisation, we focus on training and knowledge transfer, because the world today is not about technology alone, it's also about skillsets and people working with technology to make sure they get the best out of it. So we have powerful, hands-on, instructor-led training. Even in our services, we make sure we spend enough time to train and educate the client on how the incident happened and how to avoid similar incidents in future.

We also believe in a partner ecosystem—at the end of the day, it's people working with people. So, we have our teams working with partner organisations and the clients, to fill in the gaps.

What are some of the findings from Group-IB's regional threat reports?

Ransomware attacks are on the rise. The attack on infrastructure, Intellectual Property thefts, data exfiltration and so on are becoming major issues for key clients. The key observation is that ransomware attacks are becoming a lot more organised

and sophisticated, while phishing scams are becoming persistent. What this means is that top brands—whether its banking, airlines, telecom—attackers actually follow marketing campaigns and design their own similar look-alike campaigns. The major brands are being closely and constantly monitored by the attackers. This is disturbing.

However, this is not about scaring people, it's about remaining alert and vigilant. In this context, education and awareness of the end user is key, because a company can invest millions in to the latest technology, but all it takes is one wrong click to lose it all.

Group-IB launched its Threat Intelligence Centre last year. Tell us more.

Group-IB has a very mature technology in place for threat intelligence and we licence it to a number of key clients especially in the banking sector, law enforcement and the government and so on, because threat intelligence is basically the window into the threat landscape—who's targeting your company, who's targeting your partner infrastructure or equipment manufacturer and so on.

The threat intelligence centre we launched last year was a strategic move to provide more rich, local content to the region. It's great to know what's happening in the international markets between attack groups, and focus on who and what is attacking us. So, we built our own threat intelligence centre. We have Arabic-speaking analysts to develop content in conjunction with our clients so

we can come up with local content, so that we can see the threat landscape in the Middle East, in particular.

Also, ever since the launch of the company's regional HQ in Dubai, Group-IB analysts have gone to great lengths to protect the region's organisations and Internet users through the discovery of a range of threats at the hands of malicious actors.

Please tell us more about cyber resilience and how and why it's becoming a key focus area.

Cyber Resilience is the ability of an organisation to handle its own threat profile. If you're a major company, a CNI-Critical National Infrastructure-like a Telco or an Oil and Gas firm, we test your resilience against those who attack you. Attackers are ruthless—they will look closely at vulnerabilities and even attack your people—right from the VIP level. They will be impersonating your brand, spreading fake news, targeting customers with phishing scams and malicious links, and so on.

We have a methodology to assess cyber resilience in the organisation. So, we are able to tell organisations, for instance, that they are very good with their technology but are lacking in a proper team or security awareness. Security is everyone's responsibility. At one time, it used to be the sole responsibility of IT teams, but it is no longer. The consequences are also much more devastating today. So cyber resilience for us is all about testing an organisation against its attackers and seeing how resilient it is against attacks. 📌

CYBERSECURITY TOP PRIORITY AS BUSINESSES CONSIDER METAVERSE INVESTMENTS: TENABLE

BOB HUBER, CHIEF SECURITY OFFICER AND HEAD OF RESEARCH, TENABLE

Tenable, the Exposure Management company, published the results of a global study that revealed that cybersecurity is the top consideration as businesses decide on investing in the metaverse. In fact, even in a challenging global economy, concerns about macroeconomic conditions trailed behind cybersecurity worries. This sentiment underscores the rising criticality of cybersecurity in a digital economy to ensure it is a safe and secure environment for users.

The study, "Measure Twice, Cut Once: Meta-curious Organisations Relay Security Concerns Even as They Plunge Into Virtual Worlds," surveyed 1,500 IT, cybersecurity and DevOps professionals in Australia, the U.K. and U.S. The study examines how organisations are approaching the opportunities and challenges associated with building, securing and participating in the metaverse, as well as offering insights into the risks and rewards of investing in this new technology.

While still in its relative infancy, organisations have begun to explore the metaverse and its capabilities. In fact 23% of organisations have already ventured into the metaverse, and 58% plan to conduct business in the metaverse within the next year.

Less than half of respondents feel very confident in their ability to curb threats in this new environment, the metaverse poses both new and legacy cybersecurity



risks and challenges. According to survey respondents, threats that are either "somewhat" or "very" likely to take place in the metaverse include:

- Conventional phishing, malware and ransomware attacks (81%)
- Compromised machine identities and API transactions (84%)



- Cloning of voice and facial features and hijacking video recordings using Avatars (79%)
- Invisible-avatar eavesdropping or 'man in the room' attacks (78%)

In addition to the cybersecurity threats, respondents identified several major barriers to entry, including the prospect of security breaches and identity theft (34%), the lack of a clear process for data privacy (33%) and the lack of experienced security professionals to secure the metaverse (32%).

"As with any new business

opportunity, first movers have the advantage and the risk," said Bob Huber, chief security officer and head of research, Tenable. "The foundation of the cybersecurity program must be solid before making a big leap into largely unknown territory and drastically expanding your attack surface. Forward- thinking organisations that take the time and make wise investments in their security personnel and the security and integrity of their infrastructure are more likely to be successful in the metaverse or any other technology investment."

Other key findings from the report include:

- 87% of respondents are in favor of regulating the metaverse.
- Nine in 10 respondents agree that organisations need to adequately develop a cybersecurity framework prior to offering services in such a virtual environment.
- More than half (55%) of respondents said their organisation will need to invest in training their current employees about safe cybersecurity practices to support their investment in the metaverse.
- When asked about the skills required for the metaverse, respondents cited UI/UX designing, 3D modeling, blockchain and gaming development, cybersecurity and software development as important development areas. 📌

THE STUDY EXAMINES HOW ORGANISATIONS ARE APPROACHING THE OPPORTUNITIES AND CHALLENGES ASSOCIATED WITH BUILDING, SECURING AND PARTICIPATING IN THE METAVERSE.

THE CLOUD IS A GROWING TARGET FOR CYBERATTACKS: SOPHOS

■ AMONG INFRASTRUCTURE AS A SERVICE (IAAS) USERS, 56% EXPERIENCED AN INCREASE IN THE VOLUME OF ATTACKS AND 67% WERE HIT BY RANSOMWARE.





Sophos, a global leader in innovating and delivering cybersecurity as a service, has published findings of a new survey, "The Reality of SMB Cloud Security in 2022." The survey found that, among Infrastructure as a Service (IaaS) users, 56% experienced an increase in the volume of attacks on their organization when compared to the previous year, and 67% were hit by ransomware. In addition, 59% experienced an increase in complexity of attacks.

For many of these users, a lack of visibility into their infrastructure, unpatched vulnerabilities and resource misconfigurations make them susceptible to various types of attacks, including ransomware. Of those surveyed, only 37% track and detect resource misconfigurations and only 43% routinely scan IaaS resources for software vulnerabilities. What's more, 65% of cloud users reported not having visibility of all resources and their configurations, and only 33% said their organisation has the resources to continuously detect,

investigate and remove threats in their IaaS infrastructure.

"It is imperative that security is prioritised as organisations continue to adopt cloud services. This includes implementing traditional threat-based protections, as well as risk-based mitigations. Unpatched vulnerabilities and misconfigured resources are both preventable mistakes and avoidable risks that make life easier for attackers. Most attackers are not unstoppable criminal masterminds, but rather opportunistic cyberthugs looking for an easy payday," said John Shier, senior security advisor, Sophos. "However, the survey also found that more advanced IaaS users are twice as likely to report a decrease in attack impact than beginners, suggesting the appropriate defence mechanisms can go a long way in deterring threat actors. For users who need help, we recommend security services that have the 24/7 experts who can detect and quickly respond to active attacks." 🛡️

FOR MANY OF THESE USERS, A LACK OF VISIBILITY INTO THEIR INFRASTRUCTURE, UNPATCHED VULNERABILITIES AND RESOURCE MISCONFIGURATIONS MAKE THEM SUSCEPTIBLE TO VARIOUS TYPES OF ATTACKS.

CYBERCRIMINALS ATTACK USERS WITH 400,000 NEW MALICIOUS FILES DAILY

In 2022, Kaspersky's detection systems discovered on average 400,000 malicious files distributed every day, indicating a 5% growth compared to 2021. The number of certain types of threats also escalated: for example, Kaspersky experts discovered the 181% increase in the proportion of ransomware detected daily. These and other findings are part of Kaspersky Security Bulletin (KSB) – an annual series of predictions and analytical reports on key shifts within the cybersecurity world.

Kaspersky's detection systems discovered an average of 403,000 new malicious files daily over the past 10 months. By comparison, about 380,000 of these files were detected every day in 2021, demonstrating a 5% jump. In total, Kaspersky's systems detected approximately 122 million malicious files in 2022, 6 million more than last year.

Kaspersky's researchers discovered that the share of ransomware encountered daily increased by 181% compared to 2021, reaching 9,500 encrypting files per day. Among other threats, Kaspersky security solutions also detected the 142% growth in the share of Downloaders – malicious programs

that install new versions of malware or unwanted applications on infected devices.

Windows continued to be the prime target of attacks among all platforms where threat families were spread. In 2022, Kaspersky experts discovered an average of nearly 320,000 malicious files attacking Windows devices. Out of all malicious files spread, 85% of them targeted Windows. However, Windows is not the only popular platform for attackers. This year, Kaspersky's detection systems also discovered that the share of malicious files in Microsoft Office formats distributed daily doubled (236% of growth).

In 2022, Kaspersky experts also identified a 10% increase in the share of malicious files targeting the Android platform every day. So, in addition to Windows and Office files, Android users have also become some of the favorite targets of fraudsters. The infamous 2022 campaigns Harly and Triada Trojan, which ambushed thousands of Android users around the world, are prime examples of this trend.

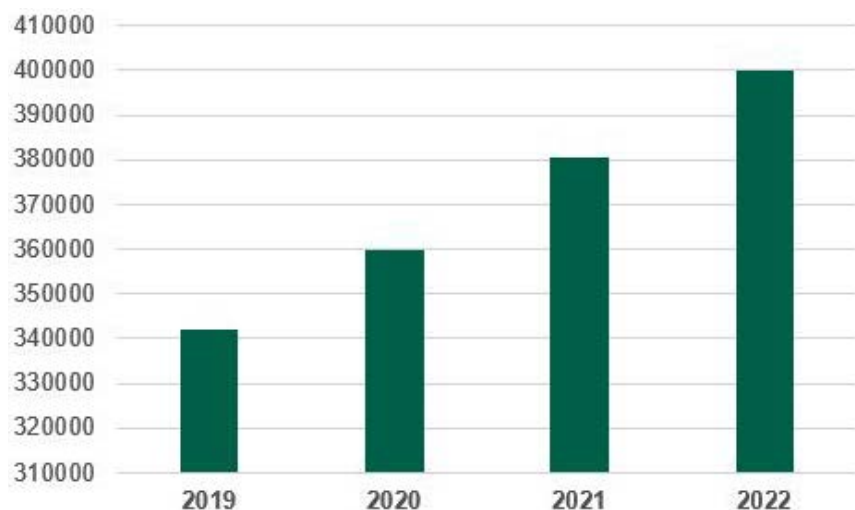
"Considering how quickly the threat landscape is expanding its boundaries and the number of new devices appearing in users' daily lives, it's quite possible that next year we'll be detecting not

400,000 malicious files per day, but half a million! Even more dangerous is that, with the development of Malware-as-a-Service, any novice fraudster can now attack devices without any technical knowledge in programming. Becoming a cybercriminal has never been so easy. It is essential not only for large organizations but also for every ordinary user to employ reliable security solutions, thus avoid falling a victim of cybercriminals. Kaspersky experts, in turn, will do their best to protect against these threats and save users from losses so that their daily online experience is completely safe," comments Vladimir Kuskov, head of anti-malware research at Kaspersky.

These findings are part of Kaspersky Security Bulletin (KSB) – an annual series of predictions and analytical reports on key shifts within the cybersecurity world. Follow this link to learn more about other KSB pieces.

To stay protected, Kaspersky also recommends users the following:

- Do not download and install applications from untrusted sources
- Do not click on any links from unknown sources or suspicious online advertisements
- Create strong and unique passwords, including a mix of lower-case and upper-case letters, numbers, and punctuation, as well as activating two-factor authentication
- Always install updates. Some of them may contain critical security issue fixes
- Ignore messages asking to disable security systems for office or cybersecurity software
- Use a robust security solution appropriate to your system type and devices, such as Kaspersky Internet Security or Kaspersky Security Cloud. It will tell you which sites shouldn't be open and protect you from malware. 🛡️





Be **data** ready.

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

commvault.com

Smart security for every home.



Ring lets you monitor every corner of your property, no matter where you are. With a Video Doorbell at your door and Security Cams around the house, you can create a Ring of Security around your entire home.

With Ring, you're always home.

ring
an amazon company

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