ADVISOR

SECONDECTOR RULE EAST



ALL ABOUT RESILIENCE

Ibrahim Azab, Regional Sales Director, MEA, CyberRes, a Micro Focus Line of Business on why cyber resilience is vital for business continuity and growth.







D-Link

p-Link

nuclias

WI-FI THAT TURBO BOOSTS BUSINESS PERFORMANCE

Indoor - Wall/Ceiling

WI-FI 6

Wi-Fi 6 Access Point



CONTENTS







06 NEWS News roundup from the world of cybersecurity

22 Gopan Sivasankaran, General Manager META at Secureworks, on the leading cybersecurity and attack trends and the company's plans for the region. 30

LLABOUT ESILIENCE

> Husni Hammoud, Managing Director at ESET Middle East, on the company's participation at GISEC and some of their cutting-edge solutions that drive demand for comprehensive security solutions across the region.

34 Mohammed Arif, Director, Modern Workplace & Security, Microsoft, on the increasing trend of the hybrid workplace.

Western Digital. WD PURPLE PRO SURVEILLANCE STORAGE when it matters most.



WD Purple[™] Surveillance Hard Drive **WD Purple™ PRO** Surveillance Hard Drive 7/24 Up to 5 years recording warranty



Capacity (Up to 18TB)

All Frame Technology Western Digital Drive Analytics



EDITOR'S NOTE



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

> Anita Joseph Editor

EVENTS



SUPERSTARS

There's only one word to describe this

issue of your favourite magazine: Superstar. It's indeed a superstar issue, packed with information and insights from the superstars of the cybersecurity field. Whether it is Zero Trust, Deterministic Protection, Threat Intelligence, XDR or Incident Response, we have it all.

To begin with, we have a cover story featuring Ibrahim Azab, Regional Sales Director, MEA, Cyber Res, a Micro Focus Line of Business, discussing cyber resilience and why it's important for business growth and continuity. FEATURING THE

We also have interviews featuring some of the shining stars of cybersecurity tell us about their participation at GISEC last month.

Our spotlight interview

with Gopan Sivasankaran, General Manager META at Secureworks focuses on the leading cybersecurity and attack trends and the company's plans for the region. Another interview with Vivek Gupta, Founder and COO, CyberKnight Technologies, discusses why Zero Trust compliance is important for complete security. Meanwhile, Mohammed

Arif, Director, Modern Workplace & Security, Microsoft, gives us the lowdown on the company's presence at GISEC 2022, its upcoming products & solutions and the increasing trend of the hybrid workplace.

That's not all. Husni Hammoud, Managing Director, ESET Middle East, throws light on some of their cutting-edge solutions that are driving demand for comprehensive security solutions across the region. Ned Baltagi, Managing Director, Middle East & Africa at SANS Institute, tells us how there is a serious shortage of skilled cybersecurity

> professionals at the global level. And finally, we have Maya Horowitz, VP Research at Check Point Software Technologies describing the company's participation at GISEC and some of the key security trends this year. One

thing is clear: The cybersecurity landscape in the region is set for a dramatic, exciting journey that's full of opportunities and challenges ahead.

So go ahead and take in all the buzz that's happening in the industry. There's not one bit in this magazine that you can afford to miss. Happy Reading!

Published by

FOUNDER, CPI ominic De Sousa (1959-2015) Do

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

EDITORIAL Editor Anita Joseph anita.joseph@cpimediagroup.comm

PRODUCTION AND DESIGN Senior Designer Analou Balbero analou.balbero@cpimediagroup.com DIGITAL SERVICES Web Developer Adarsh Snehaian

webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

© 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.

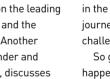
Publishing Director

Natasha Pendleton natasha.pendleton@cpimediagroup.com

Sales Directo Sabita Miranda sabita.miranda@cpimediagroup.com

OnlineEditor Daniel Shepherd

daniel.shepherd@cpimediagroup.com



EADING LIGH

THE SECURIT

INDUSTRY.

INSPIRA ENTERPRISE & MALWAREBYTES ANNOUNCE GLOBAL STRATEGIC ALLIANCE AT GISEC 2022



Inspira Enterprise India Limited has

announced a global strategic partnership with Malwarebytes, a global leader in real-time cyberprotection, to promote a robust incident response solution with Informed telemetry and sophisticated remediation techniques. Malwarebytes Incident Response is a threat detection and remediation tool built on a highly scalable, cloud-based management platform. It scans networked endpoints for advanced for malware, PUPs, and adware and removes them. Integrating with key enterprise solutions providers, Malwarebytes can conduct incident response actions-based alerts from Splunk or ForeScout solutions. With this collaboration, Inspira &

. Malwarebytes are improving threat detection, reducing the response time for threat & attack detection, with added benefits of scalability, flexibility, and automation. The inevitable GISEC 2022 is an ideal global platform for organisations to get acquainted with the next-gen Incident Response and forensics solutions for advanced threat detection and endpoint management.

ACRONIS REPORT REVEALS CRITICAL SHORTCOMINGS IN CYBER PROTECTION PRACTICES

Acronis, the global leader in cyber

protection, released its annual Cyber Protection Week Global Report 2022 timed to this year's World Backup Day. The report which surveyed over 6,200 IT users and IT managers from small businesses to enterprises across 22 countries, including the United Arab Emirates (UAE), exposes some of the most critical shortcomings appearing in cyber protection practices today, examines why they're appearing, and offers guidance on how they can be fixed. One of our key findings last year was that 80% of organisations ran as many as 10 solutions simultaneously for data protection and cybersecurity — yet more than half of them suffered downtime because of data loss. According to the report findings, the UAE performed dismally with 18% of the organisations claiming to use between 11-15 different solutions while a further 8% of companies use over 15 solutions simultaneously.

Clearly, more solutions do not translate into more protection.

This year, we see that trend getting worse: while 78% of organizations globally run as many as 10 different solutions, 76% of organisations experienced downtime due to data loss — a 25% increase from 2021. This downtime stemmed from a number of sources, including system crashes (52%), human error (42%), cyberattacks (36%), and insider attacks (20%).

KASPERSKY PATENTS BLOCKCHAIN TECHNOLOGY FOR SECURE PERSONAL DATA TRANSFER



Kaspersky's new patented

blockchain technology eases the data management process and ensures the lawful sending and processing of information. It also guarantees authentication reliability of parties involved during data transfers and ensures information confidentiality. The US Patent and Trademark Office issued a patent (US 20210021577 A1) for this technology on February 22, 2022.

The patent, "Systems and methods for sending user data from a trusted party to a third party using a distributed registry", contains methods for protecting personal data THE CONTROL OVER DATA IS ACHIEVED BY FORMING A DISTRIBUTED REGISTRY IN WHICH EACH STAGE OF THE INTERACTION IS RECORDED. from illegal transfer and processing, allowing businesses to comply with legal requirements. The technology is of particular relevance for Know Your Customer (KYC) and Client Due Diligence (CDD) service providers. Organizations can now refer to transaction records in the blockchain network to confirm parties' consent to the transfer and processing of personal data in cases of data transfer legitimacy issues.

This control over data is achieved by forming a distributed registry in which each stage of the parties' interactions during the sending of user data is recorded. The patented methods ensure that the distributed registry only contains the records pertaining to the facts of the personal data transmissions and the parties' consent to such transmissions. All records are maintained in the form of hashes that are salted, signed and encrypted in a unique, patented, way.

CHECK POINT SOFTWARE RECOGNISED AS A LEADER IN G2 GRID REPORT FOR COMPREHENSIVE SECURITY VISION

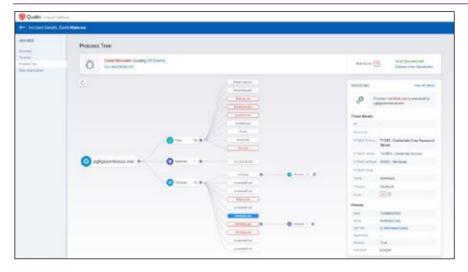
AMIT SHARON

Check Point Software Technologies

Ltd, a leading provider of cyber security solutions globally, announced that G2, the world's largest and most trusted software marketplace, has recognised it as a "Leader" across 12 categories in the G2 Spring 2022 Report. Check Point solutions secured leadership positions in next generation firewall, endpoint protection, multiple cloud security and mobile data security categories. This recognition highlights Check Point Software's continued focus on integrating cloud and on-premise security, enhancing performance and integration across its solution range, and its centralised, unified security management.

"It's an honor to be recognised as a Leader by G2 for the second consecutive year and get true user community validation and feedback," said Amit Sharon, Head of Customer Experience at Check Point Software Technologies. "Check Point's comprehensive security solutions allows for pre-emptive protection against the most advanced threats delivering uncompromised security to our customers against all forms of attacks."

QUALYS DELIVERS MULTI-VECTOR EDR 2.0 WITH ENHANCED PRIORITISATION



Qualys, Inc, a pioneer and leading

provider of disruptive cloud-based IT, security and compliance solutions, has announced Multi-Vector EDR 2.0 with additional threat-hunting and risk mitigation capabilities that improve alert prioritisation and reduce the time needed to respond to threats.

Security practitioners are inundated

with alerts, which burdens them to prioritise the ones that represent the riskiest threats, wastes their valuable time, and exposes their organisations to increased risk. Yet, traditional endpoint detection and response (EDR) solutions still focus solely on endpoint activity to detect attacks and incorporate only MITRE ATT&CK techniques – not tactics. As a result, practitioners are forced to rely on additional tools to improve their cyber risk posture leading to slow and incomplete threat remediation actions. EDR needs to evolve to scale and provide more meaningful threat context, in near real time, to meet the challenges of the modern threat landscape.

"Effective endpoint protection starts with reducing the amount and severity of instances the security team needs to address," said Michael Suby, Vice-President of research at IDC. "Qualys leverages its Cloud Platform to analyse context and data points via its integration with vulnerability and patch management along with device controls to reduce the volume of incoming incidents. This volume reduction is a key factor in saving time and resources, as it allows teams to focus on the riskiest threats that matter the most, ensuring their attack surface is less exposed."

RISKXCHANGE PARTNERS WITH BULWARK TECHNOLOGIES

RiskXchange announces a new

partnership with Bulwark Technologies to extend the reach of its cybersecurity solutions to the Middle East. Two digital security leaders will bring their expertise together to help organisations strengthen their cybersecurity posture and minimise cyber risks.

Bulwark Technologies is an established distributor of security technology and has over 20 years of experience in the IT Security market, working with customers across the entire GCC and India regions. Bulwark will bring its extensive network and knowledge of the Middle East market to the partnership.

JOSE MENACHERRY

RiskXchange will offer its integrated cybersecurity risk platform to the Middle Eastern clients. A technology which offers complete visibility and continuous monitoring of organisations' attack surfaces, including suppliers and third-party vendors, and provides companies with a more comprehensive around-theclock solution to their cyber risks.

'The prevailing crisis has paved the way for new innovations and coming-ofage technologies. We at Bulwark foresee



a spike in demand for Enterprise and third-party Cyber Risk Score Ratings and Cyber Risk Analysis solutions in the current market scenario. With RiskXchange, we are able to monitor & reduce cyber risks to provide complete and round-the-clock cybersecurity requirements of customers in the region," said Jose Menacherry, Managing Director, Bulwark Technologies.



Bedata 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

FORTINET LEADS IN SECURITY APPLIANCE SHIPMENTS FOR 9 CONSECUTIVE YEARS, ACCORDING TO ANALYST FIRM

JOHN MADDISON



Fortinet, a global leader in

broad, integrated, and automated cybersecurity solutions, has announced results from International Data Corporation's (IDC) latest Worldwide Quarterly Security Appliance Tracker. The 4Q21 Tracker and historical report data demonstrate Fortinet's continued global leadership by consistently shipping the most security appliances than any other vendor for nine consecutive years and accelerating revenue growth faster than competitors.

• During the entire year of 2021, Fortinet saw appliance shipments increase by 31.4% year-over-year, earning 36.8% unit market share for the combined firewall, UTM and VPN markets only.

· Fortinet accounts for over one-third of all firewall/UTM shipments.

• The 4Q21 IDC Tracker demonstrates that Fortinet accelerated its revenue growth for the total security appliance market year-over-year in the fourth quarter at 20.9%, outpacing the overall market growth for all vendors of 9.7%.

John Maddison, EVP of Products and CMO at Fortinet said, "Fortinet's continued leadership demonstrates strong adoption of our innovative technology solutions and overall fast growth. FortiOS is the foundation for our appliances, delivering built-in network and security convergence, dynamic network segmentation, automation, and natively integrated Zero Trust Network Access and SD-WAN capabilities. Our purpose-built Security Processing Units, or ASICs radically increase the performance, scale, and efficiency of Fortinet appliances while improving the user experience for applications across today's hybrid networks."

ATTACKERS USING LOG4SHELL VULNERABILITY TO DELIVER BACKDOORS TO VIRTUAL SERVERS, SAYS SOPHOS RESEARCH

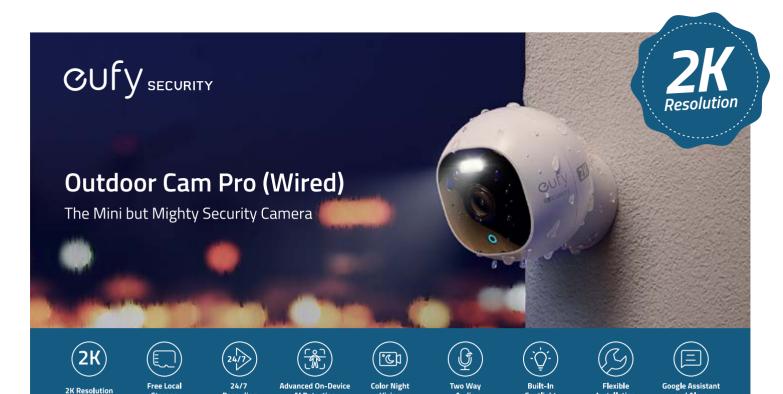


Sophos, a global leader in next-

generation cybersecurity, has released findings on how attackers are using the Log4Shell vulnerability to deliver backdoors and profiling scripts to unpatched VMware Horizon servers, paving the way for persistent access and future ransomware attacks. A new technical paper, "Horde of Miner Bots and Backdoors Leveraged Log4J to Attack VMware Horizon Servers," details the tools and techniques used to compromise the servers and deliver three different backdoors are possibly delivered by Initial Access Brokers.

Log4Shell is a remote code execution vulnerability in the Java logging component, Apache Log4J, which is embedded in hundreds of software products. It was reported and patched in December 2021.

"Widely used applications such as VMware Horizon that are exposed to the internet and need to be manually updated, are particularly vulnerable to exploitation at scale," said Sean Gallagher, senior security researcher at Sophos. "Sophos detections reveal waves of attacks targeting Horizon servers, starting in January, and delivering a range of backdoors and cryptominers to unpatched servers, as well as scripts to collect some device information. Sophos believes that some of the backdoors may be delivered by Initial Access Brokers looking to secure persistent remote access to a high value target that they can sell on to other attackers, such as ransomware operators," he added.





Storage

Recording

AI Detection

Stunning Colors and Detail

ULTRA 2K resolution and the F2.0 aperture work in tandem to produce vivid images that give you the complete picture.



Vision

Audio

Spotlight

Secure in Extreme Weather Conditions

With an IP67 weatherproof-rating, Outdoor Cam Pro boasts greater protection against the elements than any of its competitors.



nd Alexa

Subscription Free Security

Installation

Equipped with a 32GB memory card and on-device AI, Outdoor Cam Pro offers security that is ready out of the box. *The device can support up to 128G.



Notifies You Only When Needed

The camera's built-in AI accurately identifies when a person is present. This means that you are only notified when an event occurs that requires your attention.



Color Detail at Night

The built-in spotlight illuminates the surrounding area when motion is detected and allows the camera to capture footage in vivid color. Giving you a much clearer view of who's there.



Flexible Installation

The Magnetic Mount and 20ft Cable allow you to easily install the camera anywhere on your property.

AED 299/-



Available at all leading electronics stores.

CYBERSECURITY AUTOMATION: DIFFERING PRIORITIES SHOW NEED FOR BETTER C-SUITE AWARENESS

CÉLINE GAJNIK, GLOBAL MARKETING DIRECTOR AT THREATQUOTIENT

ou don't have to look far in the media to find experts predicting that 2022 will be the year of automation. As the technology skills crisis continues - and the post-pandemic

'great resignation' prompts burnt out IT professionals to consider career alternatives - it is clear that if people aren't available to plug the gaps, automation must be at least part of the solution.

Cybersecurity automation will be critical to lift the burden of high volume mundane, repetitive tasks from skilled employees creating more secure companies and attractive employment for cybersecurity professionals. In the current environment, automation is fundamental to strengthening an organisation's security posture, but there are challenges to effective implementation. We recently polled senior cybersecurity leaders to learn more about how they view automation, the challenges faced and their plans to implement it in the coming year. We found a need for better understanding of the potential of automation at C-suite level.

Perceived importance of automation varies between roles

Study found widespread recognition of the value of IT security automation and highlighted differences in opinion depending on what role the respondent had. 94% of Heads of IT Security Solutions Architecture rated security automation, important to their organisation, with 33% rating, very important. Heads of Incident Response were more likely to say automation was very important (37.5%) with a further 50% saying it is somewhat important. CISOs, however, placed less importance on automation, with a comparatively low 28% rating it very important.

These discrepancies indicate differing awareness around both the current situation within security teams and the role automation plays in driving efficiency. Incident responders are on the ground at the forefront of defence and naturally prioritise tools that ease workload, while security solutions architects are looking for tools that reduce pressure on teams while also increasing coverage. While these are undoubtedly key factors for CISOs, there is perhaps less awareness of how security automation can deliver improvements fast.

What is driving the demand for more IT security automation?

In terms of the top three drivers for adopting security automation, the three

roles agreed that increasing productivity was the most important benefit. This reflects the heavy workloads inherent in security departments and the everpresent need to do more with less by making team members more productive.

Solutions architect respondents pointed to skills shortage as a key automation driver, but respondents in all three roles also acknowledged that lack of skills has proved a barrier when implementing security automation creating a familiar chicken-and-egg scenario where organisations want to automate to solve the skills shortage, but can't because they lack required skills. For automation solution providers, this underlines the need to ensure solutions are easy-todeploy, draw together tools and data that the organisation is already using, and deliver fast ROI.

Regarding specific automation features leaders are seeking in a security product, a split was evident. More heads of incident response (IR) rated having atomic actions that take place inside one system, such as automatically creating a ticket, as critically important than did their CISO counterparts. This underlines the reactive, time-critical and high-profile nature of IR – tools must not only discover threats, but also set out the path to remediation as quickly as possible.

IR leads aren't quite ready to take their hands off the tiller entirely. On the value of "partially automated workflow automation that updates multiple systems and products, but involves human intervention to either initiate or approve the actions taken", more than one quarter of IR heads thought this was critically important, compared to just 13% of CISOs and 20% of security solutions architects. Clearly IR teams want to have visibility into automated processes and control over actions, while CISOs and solutions architects are less concerned about being hands-on.

"FOR CISOS, THE MOST IMPORTANT REQUIREMENT FOR SUCCESS WHEN ROLLING OUT SECURITY AUTOMATION IS HAVING WELL-DEFINED MANUAL PROCESSES."

Perceived success factors and barriers to security automation

For CISOs the most important requirement for success when rolling out security automation is having welldefined manual processes. This is not too surprising – CISOs are looking at the current situation and projecting forward, therefore having a good understanding of the process they are aiming to automate is important. However, CISOs shouldn't limit their automation ambition to basic direct replication of a step-by-step manual process. A security automation project offers a great opportunity to integrate other intelligence sources that can give greater context to the data and alerts received, transforming the original manual process into something far more effective. IR leads understand this; for them integration between vendor technologies was the most important requirement for success.

Looking at the blockers to implementing security automation, CISOs found management understanding/buy-in to be the biggest problem, suggesting that they need to better communicate the strategic benefits to the C-Suite in order to gain sign-off on projects. IR leads acknowledge the skills shortage, with more than half saying a lack of relevant skills is stopping them from applying IT security automation. However, skills shortages are also driving the need for automation - 43% of solutions architects say it is the reason more automation is needed.

Lack of trust in outcomes

Interestingly, the study also found that, despite the general agreement that IT security automation is important, there is a lack of trust in the outcomes delivered by automated processes. All three roles polled raised this as a problem they've encountered when implementing automation. This is akin to the "black box" problem suffered in AI, where a lack of visibility into the process makes humans less likely to trust recommendations. Security automation vendors need to consider this and ensure their solutions provide the right degree of transparency and control over alerts and policy application to engender trust. Beyond this, it is undoubtedly the case that as solutions prove themselves over time, greater trust will be built.

Our research shows that there is work to do to ensure the value of IT security automation is understood at all levels of the business. There needs to be greater alignment between the different components of IT security teams and communication from the incident responders and solutions architects up to C-suite level will help to better establish priorities.

At C-level there's a need for greater recognition of the accelerative impact security automation can have on corporate security posture. Additionally, there must be a shift in mindset away from thinking of automation projects as simply replicating existing processes, toward recognising the transformative possibilities that adding contextual information and remediation pathways can deliver.

CYBER HYGIENE: ELEMENTS TO ENHANCE YOUR CYBERSECURITY STRATEGY

IN AN EXCLUSIVE TO SECURITY ADVISOR, **DAVID BROWN** OF AXON TECHNOLOGIES EXPLAINS HOW CERTAIN MEASURES SUCH AS DIGITAL FOOTPRINTS AND NETWORK SEGMENTATION ARE OFTEN OVERLOOKED – UNDERSCORING THE NEED TO ESTABLISH A STRONGER SECURITY STRATEGY.

he security strategy of an enterprise is a blend of traditional best practices and those that it develops based on multiple other internal drivers. This could include the experience baseline of the CISO, the number and level of skilled resources available within the enterprise, the culture of the organisation, the market segment in which it operates, and lastly, its previous track record of managing cyber security incidents.

A typical list of best practices that every enterprise must follow

includes ensuring that routers and firewalls are installed and properly configured; updating whitelists of authorised users and blacklists of prohibited or unauthorised users; ensuring that anti-malware protection software is functional and correctly configured; updating all operating systems, business applications, web browsers, and firmware with latest security patches; and activating strong password rules with two factor or multi-factor authorisation procedures.

However, despite the rigorous implementation of these activities,

threats from unanticipated sources and entry points are possible.

Here are five other areas that if proactively maintained, go a long way in boosting the cyber hygiene of an enterprise.

#1 Disaster Recovery – How Quickly Can You Respond to and Recover from an Attack?

Disaster recovery processes are the foundation for a resilient security strategy. By default, backups are thought to be successful once completed but may become a source of failure at a late stage. Typically, parts of the backup process may fail and go unnoticed by administrators.

More seriously, threat actors may be successful in purging on-premises and cloud backups, while disaster recovery processes may never have included off-line backups or tape-based data backups. Going forward, best practices for disaster recovery should include routine exercises to detect backup failures and must follow the 3-2-1 backup rule.

#2 Digital Footprint – Keeping the Big Bad Wolves Away from your Door

One of the most vulnerable areas for an enterprise is leaving doors open that are facing the Internet. Typical examples include expired domain names; expired SSL Certificates; forgotten cloud servers or buckets; demo web services left running; exposed services and ports. A digital footprint audit gives deep visibility beyond a typical network boundary into areas that may provide a backdoor Internet entry into the enterprise. Knowing everything that you are exposed to will show not only where there are holes, but also where duplication exists.

Having one Windows Remote Desktop Server open to the Internet is never good but learning that you have twelve of them is eyeopening. By using security gateways and terminating nonessential and redundant Internet-facing services, the defensive profile of an enterprise is vastly improved. A well-maintained digital footprint consolidates Internetfacing assets, known and unknown, into a manageable inventory.

#3 User Policies – Clarity and Transparency Are Key to Security

The enterprise must define at an early stage what is allowed and not allowed inside the information technology and networking system. Certain practices can be detrimental to the wellbeing of an organisation's workflow and create additional challenges for administrators.

For example, unrestricted usage of the Internet for e-commerce, file storage, social media, media streaming, are mostly unrelated to business processes. Continuous usage by employees, by adding notifications and popups from third-party interfaces, cloud the cyber hygiene of an enterprise.

The enterprise must also have clearly defined policies about not allowing removable media such as USBs, external hard drives, mobile phones, and personal devices to be plugged into the enterprise network.

> "A DIGITAL FOOTPRINT AUDIT GIVES DEEP VISIBILITY BEYOND A TYPICAL NET WORK BOUNDARY INTO AREAS THAT MAY PROVIDE A BACKDOOR INTERNET ENTRY INTO THE ENTRY INTO THE ENTERPRISE."

#4 Network Segmentation – Restricted Access: Authorised Personnel Only

At one stage industrial enterprises physically separated industrial control systems and information systems. However, with industrial enterprises also adopting digital transformations solutions post-pandemic, this is no longer feasible. Enterprises need to proactively segment their networks with built-in Zero privileges, while moving from one network segment to another, as well as setting up alerts in case there is an attempt to breach these segments. Does a library PC in a remote university location need to access the central database server farm? Limiting access privileges exclusively to those who need it protects the enterprise network from widespread cyberattacks and enables better performance as it reduces the volume of users in specific zones.

#5 Data Encryption and Classification – An Organised Enterprise is a Secure Enterprise

Data should be classified based on importance and usage. Classification allows the internal security team to understand how to protect the data and locate it within the enterprise. If data is stolen from the enterprise, classification marks help to make it identifiable for the administrators. Any data that has a high classification level should be encrypted both in storage and transport. This ensures that an enterprises' most valuable data is encrypted when it is travelling across the network.

These five processes, amongst others, are critical to reduce the risks and exposure of an enterprise. It leads to a huge improvement in cyber hygiene while building a resilient security strategy. "ENTERPRISES CAN BECOME CYBER RESILIENT BY KEEPING THEIR DATA SAFE WITH IDENTITY GOVERNANCE AND ADVANCED AUTHENTICATION, VULNERABILITY DETECTION IN THEIR APPLICATIONS & PERSISTENT DATA PROTECTION."

ALL ABOUT RESILIENCE

IBRAHIM AZAB, REGIONAL SALES DIRECTOR, MEA, CyberRes, A MICRO FOCUS LINE OF BUSINESS, TELLS ANITA JOSEPH WHY CYBER RESILIENCE IS VITAL FOR BUSINESS CONTINUITY AND GROWTH.

yberRes, a Micro Focus Line of Business, is well-known for equipping organisations with cyber resiliency. What does this mean and why is cyber resiliency so important today?

Cyber Resiliency denotes the ability of organisations to anticipate threats and attacks, withstand them, recover from them and constantly adapt to the compromises and changes made to their cyber-enabled infrastructure. From securing the industry value chain to digital transformation, cyber resiliency powers and accelerates business value. It helps enterprises prepare for, respond to and recover from cyber threats so they can thrive in the face of adverse conditions (crisis, pandemic, financial volatility, and more). Until COVID-19 struck, the crisis management plan of most organisations took into account only natural disasters, however, in the days following the pandemic and the accelerated digital transformation that followed, they recognised the need for a robust cyber resilience strategy that would help them bounce back swiftly

from any kind of volatility. Today, it is well-known that cyber resilience is an invaluable asset for businesses hoping to survive and thrive, as it increases the business value of organisations and powers growth.

Enterprises can become cyber resilient by keeping their data safe with identity governance and advanced authentication, vulnerability detection in their applications, and persistent data protection. They can detect

> "CyberRes MULTI-CLOUD ENABLED CYBER SOLUTIONS REDUCE THE COST OF OPERATING A COMPREHENSIVE CYBER OPERATIONS CAPABILITY WHILE ACCOMMODATING CLOUD-NATIVE WORKLOADS AND SECURITY CONTROLS."

and accelerate threat detection and response by making smart decisions about security posture with intelligent, analytics-driven solutions. Lastly, by intelligently adapting their security infrastructure, enterprises can evolve and stay ahead of cyber threats and risks.

How does Artificial Intelligence (AI) play a role in cyber resiliency? How does it strengthen your product & solutions portfolio?

Artificial Intelligence and Machine Learning [AI/ML] are important contributors to effective cyber resilience. They help organisations go beyond the traditional 'predictive modelling' behaviour that combines historical data with real-time behaviour to understand or predict future behaviour. With the traditional approach, we can probably answer the question, "What happens next?" However, given today's complex and complicated attack scenario, our security analytics mustn't stop here, and this is where AI/ML steps in.

AI/ML provides the ideal analytics paradigm combining intelligent sensor

and ubiquitous data sources—desktops and servers, mobile, cloud, social networks, open data, etc.—with multiple advanced analytical approaches to behavioural and threat analysis, including forensic analysis, risk modelling, anomaly detection, behavioural and response optimisation, and more. This means that we can do far more than predict or identify a threat. AI/ML allows us to go even further to offer not just advanced detection but insight into how to respond most effectively. Security analytics gives us the power to answer other key questions, like "How many threats are there?" and "What is the best possible reaction?"

We've been steadily infusing our existing products with Artificial Intelligence features. These AI-based capabilities ensure that application teams can meet growing demands in an effective, efficient and agile way by increasing test coverage and test asset resiliency and reducing test creation time and maintenance efforts. Applying advanced analytics, Artificial Intelligence and data science expertise to your security solutions, the solutions within our Interset group solve the problems that matter most.

Gartner has said that going forward, cloud will be the centerpiece of all new digital experiences. How does your organisation approach cloud security?

As global organisations lift and shift workloads to the cloud, data analytics and data science rise to the top of their priority lists. Drivers for cloud migration include financial benefits like payper-use, operational benefits like zero maintenance, IT modernisation with reduced need for capacity planning and management, and technical benefits like easy availability of 3rd party data streams. There is unmet demand from

"RECENTLY, CyberRes ANNOUNCED THE ACQUISITION OF DEBRICKED, A DEVELOPER-CENTRIC OPEN SOURCE INTELLIGENCE COMPANY AIMED AT INNOVATING HOW ORGANISATIONS SECURE THEIR SOFTWARE SUPPLY CHAIN."

the business as on-premises data centers only serve a small percentage of the actual demand for data analytics. Platforms for Machine Learning and Artificial Intelligence are readily available in the cloud and offer the potential to discover new value and insight using large stores of business data.

Our CyberRes solutions and integration partners enable enterprises to secure their cloud environment from design to development. We enable risk awareness, access, transparent data protection, continuous security, and real time cyber defence with realtime analytics. CyberRes Security offerings enable business owners to ensure necessary privacy, security, and compliance practices that protect cloud assets, identities, applications, and services comprehensively and, in turn, build a stronghold of trust. CyberRes multi-cloud enabled cyber solutions reduce the cost of operating a comprehensive cyber operations capability while accommodating cloudnative workloads and security controls.

A collaborative approach is being considered the best way to tackle the growing threat landscape. How do you think industry stakeholders can come together to make cyberspace a safer place?

When it comes to cybersecurity, effective collaboration means concerted effort from all stakeholders about various effective cyber defence techniques. Businesses are increasingly beginning to realise that a disparate or fragmented approach to security operations is ineffective against the ever-growing. sophisticated threats that we're seeing today. It is now well understood that only a collaborative approach that encourages strong partnerships will bring together all the disconnected parts and help organisations put up a stronger front against the complex landscape of today and the attackers of tomorrow.

2022 is the year to come together and implement effective changes to prevent future attacks from happening. A zero-trust architecture can (and will) help CISOs across different industries to better protect their companies and focus on new problems, innovations and challenges beyond cybersecurity. Another critical need to help bring more resilience is deeper and more meaningful insight and actions from threat data. CyberRes recently launched Galaxy, which gives CISOs to analysts an immersive threat research experience that can be customised to the needs and industries of every user. This is a great way to help bring data insight and best practices to the security industry.

What does CyberRes have in store for 2022?

There are several areas of focus that CyberRes has for this year, including cloud/SaaS solutions spanning all four portfolio areas (ArcSight, Fortify, NetIQ,



and Voltage), as well as addressing major issues facing security teams, such as securing supply chain and industry needs. In addition, we have exciting innovations coming up, not just within our product portfolio, but also within Galaxy as it continues to grow.

In this context, it is worth mentioning Micro Focus's CyberRes Galaxy Threat Acceleration Program Basic and Plus (GTAP/GTAP+) here. GTAP+ is an intelligence feed built specifically curated for use with ArcSight Enterprise Security Manager (version 7.6). It is the premium Threat Intelligence solution component of the CyberRes Galaxy platform and incorporates insights from Galaxy's threat research network to provide ArcSight customers with proactive defences. Along with the GTAP+, there's also GTAP Basic-a free-of-charge add-on for existing ArcSight ESM customers, composed of the public Threat Intelligence feed instance of the MISP CIRCL open-source intelligence solution.

Recently, CyberRes also announced the acquisition of Debricked, a developer-

"OUR CyberRes SOLUTIONS AND INTEGRATION PARTNERS ENABLE ENTERPRISES TO SECURE THEIR CLOUD ENVIRONMENT FROM DESIGN TO DEVELOPMENT."

centric open source intelligence company aimed at innovating how organisations secure their software supply chain. Debricked's SaaS solution allows for a more intelligent selection of open source while drastically reducing the risks typically associated with it, both core requirements of modern DevSecOps programs. The service is powered by state-of-the-art machine learning which enables the data quality to be extremely accurate as well as instantly updated whenever a new vulnerability is discovered. What makes Debricked unique in the world of open source security is its high level of precision. combined with developer focused UX and unique abilities to customise the service to a company's needs.

In addition, the Fortify on Demand (FoD) delivers application security as a service, providing customers with the security testing, vulnerability management, expertise, and support needed to easily create, supplement, and expand a Software Security Assurance program.

Fortify Hosted provides a cloudbased enterprise service for automating application security programs. It enables management, development, and security teams to work together to triage, track, validate and manage software security activities. Fortify Hosted enables Static Application Security Testing (SAST), Dynamic Application Security testing (DAST) and optionally Software Composition Analysis (SCA) to be fully integrated into the Customer's Software Development Lifecycle. Micro Focus is responsible for the provision of Fortify Hosted on an AWS or Azure cloud platform and delivers ongoing infrastructure, application and support service remotely.

In short, 2022 began on a strong note for us and we're excited about what the rest of it has in store.



EVERDOME

The Digital Frontier's First Hyper-realistic #Metaverse

Everdome aims to create the most hyper-realistic metaverse that will bring brands and people together - all with the intent of building the most realistic web3 experience.

See whats waiting for you...



WWW.TAHAWULTECH.COM

ISSUE 64 | APRIL 2022





🔅 tahawultech.com



POISED FOR GROWTH

GOPAN SIVASANKARAN, GENERAL MANAGER META AT SECUREWORKS, SPOKE TO ANITA JOSEPH ABOUT THE LEADING CYBERSECURITY AND ATTACK TRENDS AND THE COMPANY'S PLANS FOR THE REGION.

hat products/ solutions did you showcase at GISEC this year? At GISEC, we

primarily discussed SOC of the future, how organisations can continuously improve the efficiency and effectiveness of SOC operations. We also discussed the following key areas:

• What does the threat landscape look like in 2022 and how is it evolving in a way organisations need to make a change in their cybersecurity strategies?

• Some of the key challenges organisations face in protecting themselves from these ongoing threats stem from the fact they lack full visibility across their own entire IT and security infrastructure and not having enough cybersecurity skills in-house to protect themselves.

• And finally, we showcased our award-winning, battle tested platform Taegis, which has been built by security experts for security experts to prevent, detect, and respond to threats and vulnerabilities.

What are the leading cybersecurity trends this year?

It's extremely difficult to be a cybersecurity buyer in today's world, mainly because it's easy to get lost in the sea of similar-sounding language and difficult terminologies like EDR, MDR, and XDR.

And threats continue to evolve.

One thing I can say for sure - **XDR will** take centrestage in 2022

While the XDR (extended detection and response) market is still relatively young, we can expect it to take center stage in 2022. With limited visibility into their hybrid IT environments, understaffed security teams, and growing cost and complexity of managing disparate security tools, organisations are increasingly looking at XDR solutions to unify their existing security infrastructure, provide actionable, focused insight from a single console so that security teams can investigate and rapidly respond to threats in a highly automated and rapid fashion. XDR solutions provide

that comprehensive attack surface coverage across endpoint, network, identity and cloud environments to help organisations gain a full understanding of the threat scenario and quickly respond accordingly.

Organisations will increasingly turn to MDR (managed detection and response) to gain efficiencies

With the scarcity of skilled cybersecurity talent and the fact that many organisations lack sufficient resources, organisations will increasingly be looking at Managed Detection and Response (MDR) services. Many organisations cannot afford to build and operate their own SOC or hire a dedicated security team to provide the 24x7x365 threat monitoring and response coverage need to stay ahead of an evolving threat landscape. Organisations that do have security staff but are looking to scale up, will also turn to MDR service providers to expand their capabilities. According to Gartner, by 2025, 50% of organisations will be using MDR



services for threat monitoring, detection, and response functions that offer threat containment and mitigation capabilities (source: Gartner).

Automation and Risk-Based Prioritisation will become key to Vulnerability Management

Vulnerability management continues to be ineffective because the issue of prioritisation continues to be ignored. Security teams have been detecting vulnerabilities over the years and passing these to the IT teams to patch, and we have now got to a stage where the IT teams are potentially expected to patch thousands of vulnerabilities every day. By the time they get closer to the target, the next set of vulnerabilities arrive. On top of that, there are severe dependencies on underlying application support, downtimes, etc. The only way we can solve this problem is by having an effective and automated way to prioritise vulnerabilities to bring the number to practical numbers instead of thousands. Al technology

is one approach that can help alleviate the exploding burden on typical vulnerability management operations teams and we can expect to see an increase in the use of Al in the detection, prioritisation and remediation of vulnerabilities. Relying on vulnerability severity scores is no longer effective and organisations will have to shift towards prioritisation based on the context of the environment. As such, organisations will be looking for technologies that can guickly assess and determine what should be prioritised based on the likelihood of a vulnerability being exploited times the potential impact on the organisation and its overall business. Understanding the risk posed by vulnerabilities to an environment will be key to vulnerability management in 2022.

What is 2022 looking like for Secureworks and what is your major area of focus going to be?

We are expanding in the region to meet increased customer demand. I took on

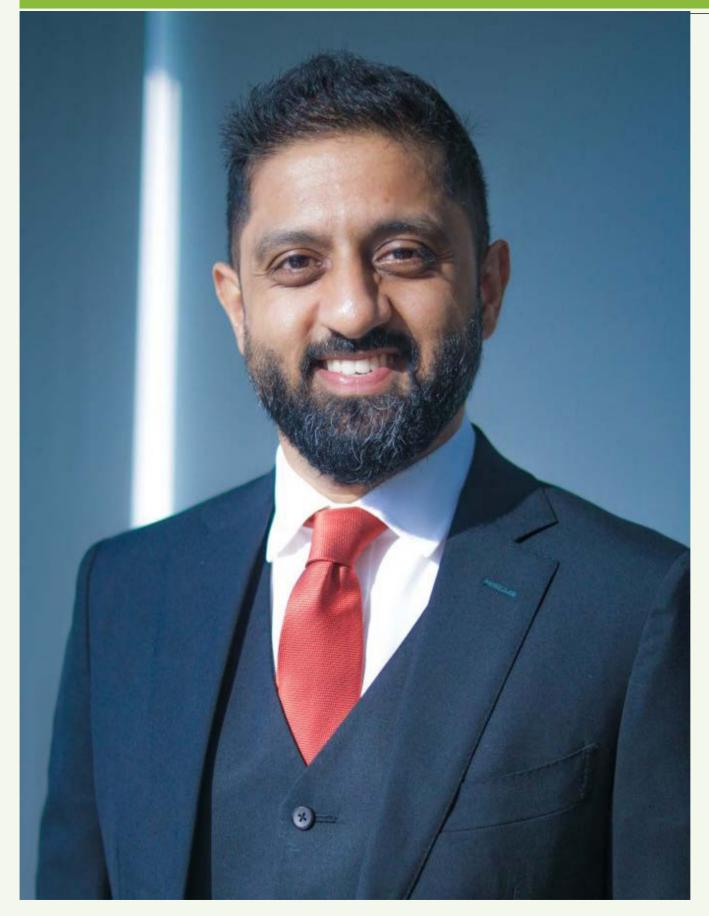
the leadership role for Secureworks in the META region in August 2021, and we are building out our sales, marketing and service delivery teams in the region. This region is a fastgrowing market, so we're absolutely committed here. Our focus will be centered around bringing Taegis to mass market throughout the region.

The channel continues to be an important business driver for us in the region, and we will continue to maintain focus there. Our recent distribution agreement with Redington reinforces our commitment to the channel.

From a geographic coverage perspective, our focus has been primarily in GCC, and we are now bringing focused attention to the African market with new teams dedicated for South Africa and Emerging Africa.

It's not just 2022 that we are looking at in terms of growth. We plan to grow Secureworks' market presence through consolidation and expansion plans over the next few years.

GISEC SPOTLIGHT / CYBERKNIGHT TECHNOLOGIES



NAVIGATING THE PRECARIOUS CYBERSECURITY LANDSCAPE

AVINASH ADVANI, FOUNDER & CEO, CYBERKNIGHT TECHNOLOGIES, ON THE THEME OF THEIR SHOWCASE AT GISEC 2022 AND THE MAIN CYBERATTACK PATTERNS TODAY.

hat was the theme for this year's GISEC? The theme was Business Interrupted: Navigating the Precarious Cybersecurity Landscape, which is an obvious theme given the geopolitical landscape that we're currently operating in. As we know, a lot of warfare these days is fought online and so it's a very relevant theme.

What are the technologies you showcased at GISEC?

We have 14 different vendors at our stand, who represent a cross-section of the entire portfolio. We're very focused around the important theme of Zero Trust security and so all the vendors at the stand contribute in some way to this. What's important is that all the vendors at the stand really represent the Zero Trust Security story.

*DURING THE PANDEMIC, THERE WAS A MASSIVE RISE IN RANSOMWARE WHICH KICKED OFF AND HASN'T STOPPED OR SLOWED DOWN."

What are some of the main attack patterns that we're seeing post the pandemic?

There are two facets to this: One is that during the pandemic, there was a massive rise in ransomware which kicked off and hasn't stopped

or slowed down. We started to see a lot of supply chain issues during the pandemic, but we've come to grips with this because people have started to realise the need to stay secure against ransomware. But we hear less about ransomware attacks. Today, the main issue is the Russia-Ukraine crisis, where anyone that has a direct or indirect link to either country is at risk, because they become part of that supply chain. If you think about how big that scope is-whether it is Retail, FMCG, Oil & Gas, Energythe list is huge. So the same supply chain issue that began last year because of ransomware, continue today, not because of ransomware, but because of the ongoing crisis. So, it's a continuation of the trend, but a softening of the ransomware factor and more because of the ongoing crisis and its impact on the supply chain. 🚦

GISEC SPOTLIGHT / CHECK POINT SOFTWARE TECHNOLOGIES



CONCERTED EFFORTS NEEDED TO PREVENT CYBERATTACKS

MAYA HOROWITZ, VP RESEARCH AT CHECK POINT SOFTWARE TECHNOLOGIES SPOKE TO SECURITY ADVISOR ABOUT THE COMPANY'S PARTICIPATION AT GISEC AND SOME OF THE KEY SECURITY TRENDS THIS YEAR.

hat did it mean to be participating at GISEC this year? It was exciting to be a part of GISEC this year-to be able to hear and talk to so many people and exchange ideas on cybersecurity. GISEC is a great forum that brings together all the frontrunners in the field.

What are the products and solutions you showcased at GISEC?

It is extremely necessary to adopt a consolidated security architecture for businesses looking to enhance their cyber security posture across platforms – from edge to cloud. At this year's GISEC, Check Point Software emphasised the new strategic "GLOBALLY, RANSOMWARE HAS IMPACTED HOSPITALS' ABILITY TO PROVIDE CRUCIAL SERVICES, CRIPPLED PUBLIC SERVICES IN CITIES, AND CAUSED SIGNIFICANT DAMAGE TO VARIOUS ORGANISATIONS." direction, 'You Deserve the BEST Security' and showcased our broad range of security solutions designed for today's dynamic business environment.

According to Checkpoint's global research, what are some of the leading cybersecurity trends that we're seeing this year?

Ramsomware is very much prevalent and is the most important threat that we're seeing, continuing from the previous year. Ransomware has quickly become the most prominent and visible type of malware. Globally, ransomware has impacted hospitals' ability to provide crucial services, crippled public services in cities, and caused significant damage to various organisations.

INCIDENCE RESPONSE-THE SECRET TO STRONG CYBER RESILIENCE

KAPIL MATTA, REGIONAL MANAGER, ENTERPRISE AT MALWAREBYTES, ON WHY THE KEY TO GOOD CYBER RESILIENCE IS INCIDENCE RESPONSE.

t felt great to be at GISEC, a truly global event for cybersecurity in the region, said Kapil Matta. In his opinion, participating in the event in 2022 was special because the who's who of the cybersecurity were able to meet up again and exchange ideas and information face-to-face.

According to him, Malwarebytes has been leveraging years of security experience in remediation to provide customers with threat intelligence from millions of Malwarebytesprotected endpoints, across both business and consumer endpoints. "Malwarebytes Endpoint Protection,

managed within our own cloud-native

Nebula console, easily scales to meet future requirements. It effectively and efficiently detects suspicious activity, prevents attacks and removes malware infections. Other solutions can be difficult to deploy and manage, and only remove malware executables, leaving damaging artifacts and configuration changes behind. Because of less effective classification machine learning models, other solutions can have high positive alerts that burden analysts and security teams and prevent accurate detections. Malwarebytes has won several industry-wide awards and accolades for its effective detection with low false positives."

In his opinion, incident response is an important key to cyber resilience.

"While strong prevention is crucial, organisations must also have strong capabilities to detect and remediate attacks that can get through even the best defences. Minimising dwell time is critical to minimising damage and an area where organisations need to focus optimising their incident response processes."

"According to incident response (IR) teams, malware is the root cause of 68% of the incidents they investigate. But how long does it take to recover from these attacks? When an attack occurs, security best practice recommends meeting the



1-10-60 rule: 1 minute to detect, 10 minutes to investigate, and 60 minutes to remediate. However, the reality is that security operations center (SOC) teams require days to weeks to eradicate an incident.

Matta pointed out that automation tools are a key contributing factor behind increased response time efficiency. In fact, 25% of incident responders list full automation of detection, remediation, and follow-up workflows in their 12-month plan for incident response improvements.

"IR automation requires parting ways with the traditional reimaging processes. While reimaging an infected endpoint has a long "AUTOMATION TOOLS ARE A KEY CONTRIBUTING FACTOR BEHIND INCREASED RESPONSE TIME EFFICIENCY. "

legacy as the de facto standard, it's fraught with time inefficiencies and inherent risks. This adds up to hours of restoring endpoints and lost productivity caused by employees. There's also a high likelihood of lost work caused by the time between the last clean backup and the time of infection. The net result of this is a loss of employee productivity and ultimately money," he added. In conclusion, Matta shared, "By compressing response times with fast and complete remediation and API integration across organisations' security stack, enterprises can drive further automation and orchestration while bolstering cyber resilience." 1





ESET: INNOVATING FOR GREATER SECURITY

HUSNI HAMMOUD, MANAGING DIRECTOR AT ESET MIDDLE EAST, ON THE COMPANY'S PARTICIPATION AT GISEC AND SOME OF THEIR CUTTING EDGE SOLUTIONS THAT DRIVE DEMAND FOR COMPREHENSIVE SECURITY SOLUTIONS ACROSS THE REGION.

hat did it mean to be participating at GISEC this year?

This is the year where we're almost done with the pandemic and people are starting to move out freely and meet each other face to face. We were able to meet and interact with our partners, customers and colleagues. GISEC has always been most important security event in the region. In fact, the response this year was enthusiastic, it looked like we might have seen a return of pre-pandemic levels of participation and interest.

What products and solutions did you showcase at GISEC?

There's a lot of innovation in security happening these days and ESET is one of the major players providing cuttingedge security products & solutions. At GISEC, ESET is presenting its APT solutions that have been witnessing rapid adoption across organisations of all sizes and industry segments. ESET is also showcasing ESET Inspect, the XDR-enabling component of the ESET PROTECT platform helping enterprises protect against advanced persistent threats, and securing them from zero-day threats and highly targeted malicious attacks. The solution bundle offers granular visibility, risk assessment, incident response, investigation and remediation helping IT security professionals to strengthen the cybersecurity posture of the organisation.

ESET, with a strong portfolio of APT solutions, neutralises advanced

ESET, WITH A STRONG PORTFOLIO OF APT SOLUTIONS, NEUTRALISES ADVANCED PERSISTENT THREATS AND THE COMPANY HAS EARNED A DISTINCTION IN 2022 FOR BEING NAMED THE 'TOP PLAYER' IN THE RADICATI ADVANCED PERSISTENT THREAT MARKET QUADRANT FOR THE THIRD TIME IN A ROW. persistent threats, and the company has earned a distinction in 2022 for being named as the 'Top Player' in the Radicati Advanced Persistent Threat Market Quadrant for the third time in a row, achieving the best position among all Europe-based security vendors.

What are some of the main security trends we are seeing this year?

Digital transformation has accelerated in the last couple of years post the pandemic. The attack vectors have also evolved and ransomware has emerged as a major threat. Identity theft and phishing are also rampant. Everyone needs 'total' solutions these days, and each security solution becomes a piece of the puzzle that we need to work on. We must also pay attention to perimeter protection where we need to look at endpoint security, classify our data and secure our access at every point-right from single sign-on to Zero Trust-all of these need to be taken care of, to prevent critical data and infrastructure.

We also need to work on our people and make sure they understand the risks and how to protect themselves, their company and critical data.

^CSECURITY IS EVERYONE'S RESPONSIBILITY

ASHRAF KOHEIL, REGIONAL SALES DIRECTOR MEA AT GROUP-IB, ON THE COMPANY'S THREAT RESEARCH FINDINGS AND ITS APPROACH TO CYBER RESILIENCE.

ell us about Group-IB's participation at GISEC. What were some of the key products and solutions you were highlighting at the

event?

This was Group-IB's second year at GISEC. As compared to last year, this year the participation was phenomenal, due to a few main reasons. One is the easing of restrictions, second, the increased focus and priority on cloud migration and then, the resounding success of the Expo. We saw considerable engagement and traction this year, newer technologies and lots of new companies in the region.

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

AT GROUP-IB, WE BELIEVE THAT CYBERSECURITY IS ALL ABOUT HAVING A COMPLEMENTARY AND AGILE ECOSYSTEM.

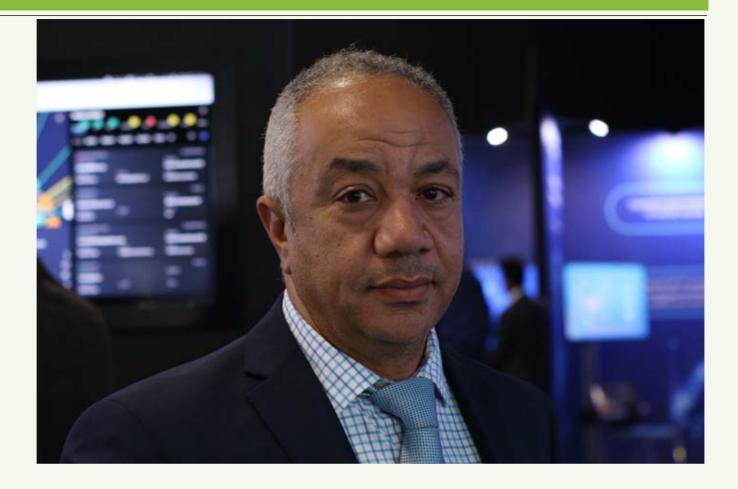
your environment from good to great or great to excellent.

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, handson, 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 ecosystemat 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.

Tell us about the launch of Group-IB's Threat Intelligence Centre last year.

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.

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. **1**

MICROSOFT: Securing The Hybrid Work Landscape

MOHAMMED ARIF, DIRECTOR, MODERN WORKPLACE & SECURITY, MICROSOFT, ON THE COMPANY'S PRESENCE AT GISEC 2022, ITS UPCOMING PRODUCTS & SOLUTIONS AND THE INCREASING TREND OF THE HYBRID WORKPLACE.

hat products and solutions did you showcase at GISEC 2022?

This GISEC, we are focused on helping customers update their security strategy to tackle two key trends that we continue to see in the market today: one, the rapid explosion of hybrid work and two, the rapidly evolving security landscape. There are new threat vectors now, and it's more complex and disruptive. What's happening is that with both of these aspects coming together, there's a whole new set of security challenges. Customers who wish to digitally transform, are realising that there's no digital transformation without security transformation. So, this GISEC, we're focused on helping customers make that security



transition with focus on securing multiple cloud and security of connected devices.

With hybrid work gaining so much traction, what products & solutions does Microsoft have, to tackle this trend?

With the rapid adoption of Teams as a key part of how customers embrace and adopt remote work, we



continue to build on that baseline technology. A big area of focus for us is employee experience. Today, when you think about how work happens, the digital employee experience is THE employee experience. These days, the first time an employee gets to know more about a company is through the digital interface. We have a suite of technologies called Viva, which is focused on the employee experience. It tackles everything from employee well-being, to employee skilling and learning.

How can you ensure the security of connected devices in a hybrid work environment?

We have a range of technologies that enable customers to be more secure. We have secure devices like the Surface range of devices and many more. But I think the No 1 advice we have for customers is to ensure that they have a Zero Trust architecture for their enterprise. Zero Trust is the global Gold standard for enterprise security. So you want to ensure that you're provisioning trust and provisioning access just in time and just enough. That is a key part of everything that we do with customers.

RISKXCHANGE: ADDRESSING SECURITY RISKS

DARREN CRAIG, CEO AT RISKXCHANGE, SPOKE TO SECURITY ADVISOR ABOUT ITS SECURITY OFFERINGS & PARTNERSHIP WITH BULWARK.

It felt great to be participating at GISEC, especially this year, when most pandemic-induced restrictions were eased and

we were all free to meet and greet physically," Darren said.

Darren is the CEO of RiskXchange, the only platform that provides a complete 360-degree view of the attack surface, including that of the vendors. Its USP is that it will continuously monitor the complete attack surface, highlight any risk and enable you to fix any issues before the attacker discovers them. "RiskXchange's integrated cybersecurity risk platform helps you discover, continuously monitor and reduce the risk across your enterprise and supply chain," Darren said. "Attackers use leaked credentials data to take over employee's accounts with privileged access. These could be the accounts of board members, senior executives, developers, and systems administrators. The RiskXchange Account Takeover Prevention system can detect and alert these corporate

credential exposures to help protect the organisation and stop attackers using leaked credentials to gain entry into the company's accounts and systems", he added.

About Dark Web monitoring, he said: "Data exposure is inevitable. RiskXchange prevents your company from a data breach online by continuously monitoring a wide range of open, deep, dark web sources, including closed sources, used by attackers that target organisations. The

"RISKXCHANGE PREVENTS YOUR COMPANY FROM A DATA BREACH ONLINE BY CONTINUOUSLY MONITORING A WIDE RANGE OF OPEN, DEEP, DARK, WEB SOURCES."

RiskXchange Dark Web Monitoring system delivers accurate, actionable and configurable alerts, that will empower your security team to stop attacks by identifying threats before they impact your business." RiskXchange was at GISEC at the Bulwark stand, where the pioneering Value-Added Distributor joined hands with its strong cybersecurity specialised vendor portfolio for the event. Accordingly, the company is offering the latest technologies spanning Digital Risk Protection, Hardware Security Modules, Encryption, Smart ID/PKI Solutions, Web Application Vulnerability Scanner, Data Classification, Data Loss Prevention, Secure Managed File Transfer, Encrypted Flash Drives & Disc Drives, Email Security & Archival, PIM/PAM, Secure Remote Access/Workspace Virtualisation, Insider Threat Prevention, Employee Monitoring, Enterprise Mobile Management solutions, Cyber Skills Development / Training platform, SIEM in addition to their other security technologies at the event. 1



BRIDGING THE SKILLS GAP

NED BALTAGI, MANAGING DIRECTOR MIDDLE EAST & AFRICA AT SANS INSTITUTE, SPOKE TO SECURITY ADVISOR ABOUT THE COMPANY'S PRESENCE AT GISEC AND HOW THERE IS A SERIOUS SHORTAGE OF SKILLED CYBERSECURITY PROFESSIONALS AT THE GLOBAL LEVEL.

hat products and solutions did SANS showcase at GISEC?

SANS showcased a vast range of its

offerings, from core training courses, Capture-the-Flag events (CTFs), security awareness products, knowledge assessments, NetWars tournaments and Cyber Training academies, to educate visitors on how SANS can support organisations in training, recruiting, and retaining cybersecurity staff. We had many products to offer organisations – small and large – to help them provide their staff with the best possible training experience. We were also there to prove that SANS is not just for experts, it's even for youngsters who are getting started in the field.

Visitors had the opportunity to experience the SANS Secure Middle East 2022 training course, which took place in Riyadh, through their Live Online training format.

At our stand, senior executives and

"SKILLS SHORTAGE IS AN ONGOING ISSUE AND OVER THE LAST TWO-THREE YEARS, IT HAS BECOME A BIGGER PROBLEM."

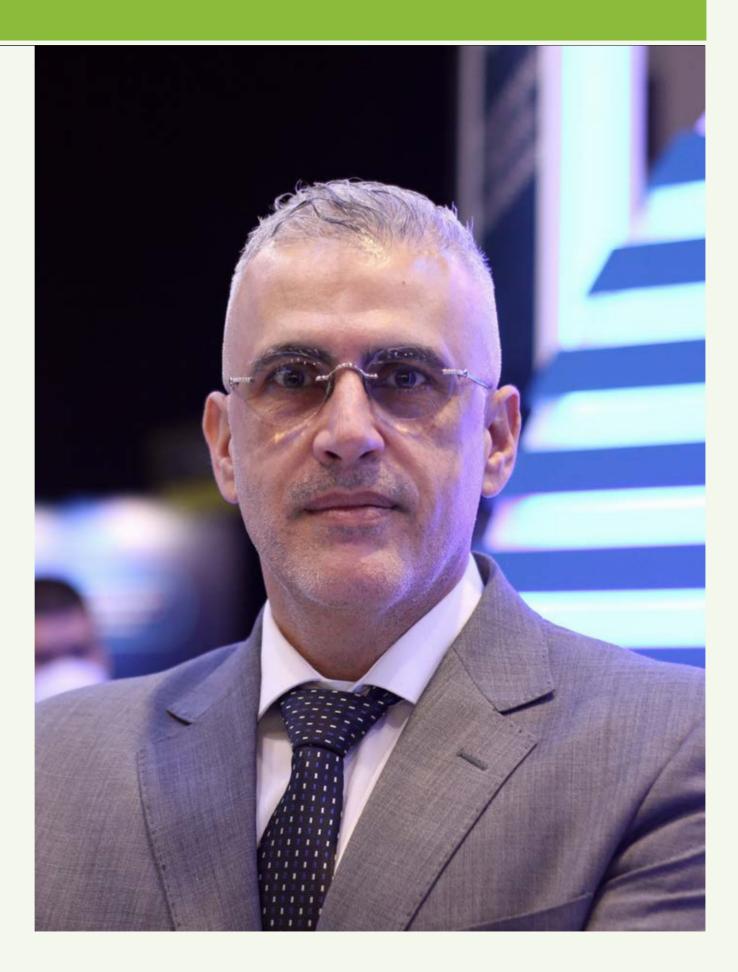
cybersecurity experts from SANS Institute were available to network and share insights on how SANS is working to bridge the current cybersecurity skills gap, as well as how individuals and organisations can adequately protect themselves against the latest cyber threats coming in from nationstate actors.

There's always been a serious shortage of cybersecurity professionals world over. Are we any closer to bridging the gap?

It's an ongoing issue. Over the last two-three years, the issue's become a bigger problem, especially with so many people staying in their current jobs and many new cybersecurity roles becoming available, especially with what's going on in Ukraine and Russia. There's an increasing demand for cybersecurity practitioners. A lot of organisations and clients are struggling with this, so I'd say the challenge now is to not just look outside the organisation, but inside the organisation and there are several different ways of doing that and we have several solutions to help organisations do that. Interestingly, this problem is forcing organisations to be creative about how to recruit talent and retain talent.

What's the threat-security landscape been looking like in the last two years?

A lot of threats have stayed the same; ransomware is bigger than before. Now, with the conflict in Ukraine, there is an increasing number of nation state attacks coming in from that region. But what we're seeing is that they're a strong community and are quickly rallying together and creating a formidable force. We're also starting to see and be concerned about destructive malware coming from the region. We're trying to ensure that everyone gets the right tools and resources available so that they can combat this threat. **1**



HIGHLIGHTING DETERMINISTIC PROTECTION

BOBBY GUPTA, SENIOR VICE-PRESIDENT AND MD OF INTERNATIONAL BUSINESS AT VIRSEC, ON THE COMPANY'S PARTICIPATION AT GISEC THIS YEAR AND HOW DETERMINISTIC PROTECTION CAN BETTER SERVE IT INFRASTRUCTURE.

hat was VIRSEC's focus at GISEC this vear? We launched our Deterministic Protection Platform (DPP) a couple of months back. DPP is the next evolution of the company's flagship and awardwinning Virsec Security Platform (VSP), the first solution that could eradicate threats to the software workload at runtime in real-time. This is what we highlighted at GISEC this year. With DPP, Virsec demonstrated how security response can be made obsolete by improving the protection that conventional, probabilistic solutions do not.

"DPP NOT ONLY ENSURES AUTOMATIC PROTECTION AGAINST ALL KNOWN AND UNKNOWN THREATS, BUT IT ALSO REDUCES ADVERSARY DWELL TIME FROM MINUTES TO MILLISECONDS."

What's the cybersecurity landscape like today, and what are some of the commonly prevalent threats?

During the pandemic, we witnessed a surge of increasingly sophisticated cyberattacks, and the rate continues to grow. Ransomware is continuing to increase. Hackers are becoming smarter and they are now targeting those areas where there was no specific attack pattern in the past. So, how can you stop attacks that have no pattern? No Al? While the industry is figuring this out, the hackers are moving fast ahead.

Virsec has a unique strategy. We don't rely on traditional ways of securing software, which we call Architecture 3.0. If you think about it, there was



endpoint security/network security, then came Machine Learning, and now we're talking of runtime protection. And since Virsec is focused on runtime protection, we're unique.

Tell us more about Deterministic Protection and how it helps companies protect their critical IT infrastructure?

DPP not only ensures automatic protection against all known and unknown threats to vulnerable workloads, but it also reduces adversary dwell time from minutes to milliseconds, specifically protecting against ransomware, remote code execution, supply chain poisoning, and memorybased attacks – with true protection and runtime observability. Combining the broadest attack coverage and highest accuracy in the industry, DPP by Virsec protects server workloads across the entire runtime stack, eliminating false positives, when deployed on bare metal, virtual machines (VMs), containers, or in the cloud. This deterministic approach to security ensures precision protection for legacy unpatched workloads, reducing, or entirely negating, the need for patching.

We're the only ones doing this, no one else is, and Virsec has a patent technology for this – we call it AppMap. Deterministic Protection has been our focus and we launched it last year. Since then, we've been seeing huge demand for this solution from clients in critical sectors.

Tell us about Virsec's global presence and growth.

Virsec is based in California, and we have our offices in India as well. Our US operations are based in Boston, Arizona, Chicago and San Jose. I'm based in California, but I run international sales. Outside the US, our key markets are Australia, India, Japan, Middle East-Africa and the UK.

The Middle East market is very important for us, since there's a lot of demand for critical infrastructure solutions here, particularly postpandemic. In fact, it's been a key market for us for a long time.

AUTOMATING Security

BOB LAYTON, CHIEF CHANNEL OFFICER, ESENTIRE AND **AMIT KUMAR,** MANAGING DIRECTOR, MMA INFOSEC, SPOKE TO SECURITY ADVISOR IN AN EXCLUSIVE INTERVIEW ABOUT AI, AUTOMATION, XDR, MDR, PREVENTION & INVESTIGATION.

s AI & Automation the way forward in security?

Absolutely. Al & Automation are indeed the way forward. Security is a data problem and if you believe it is, like we do, then you need a platform to make sense of all that data. Ours is called Atlas and it is an XDR platform that makes MDR3 – Response, Remediation and Results – possible and sorts through all the data. Patented machine learning eliminates noise, enables real-time detection and response, and automatically blocks known and unknown threats. So yes, AI & Automation are needed to keep pace with the cybersecurity threats today.

XDR or MDR-where should enterprises invest in, today?

There's so many different definitions doing the rounds. So basically, XDR is a multi-telemetry platform and MDR is something that's been around for a while. Managed Detection has been



around for 20 years; response is the hard part. And in order to have a really rich 'R' which is the response, you have to have the multi-telemetry, which is XDR.

What's the best approach-prevention or investigation?

Both are necessary because it is impossible to protect yourself from everything that happens. However, you must have a really strong preventive mechanism in place and then if something goes wrong you must be

AI & AUTOMATION ARE NEEDED TO KEEP PACE WITH THE CYBERSECURITY THREATS TODAY.

able to investigate it-whether you have compliance needs, or cyber insurance risk needs, you really have to take care of both of these aspects.

What are your plans for the region this year?

We're very excited about the Middle East region-all of the countries here. We're looking at investments in bringing our platform into the region into both cloud and on-prem locations. We're absolutely committed to the region in every way.

DIGITAL TRANSFORMATION FRONTRUNNERS

SUNIL TITTO, DIRECTOR-CUSTOMER SUCCESS AT ACCOPS, SPOKE TO SECURITY ADVISOR ABOUT THE COMPANY'S PARTNERSHIP WITH BULWARK AND ITS SHOWCASE AT GISEC 2022.

It was a matter of great pride to have participated in a global event like GISEC 2022, said Sunil Titto. "Being in the Zero-Trust space and the digital/

work-from home realm, this is a great opportunity to see for ourselves the latest innovations and trend in the sector and exchange ideas and best practices with great minds," he said.

About the company's partnership with Bulwark, Titto said that they have a long and stable relationship with Bulwark. When we decided to enter the Middle East region, Bulwark connected with us and we were able to make some potential leads and attract key customers. So, yes, the relationship has been very fruitful and growing from strength to strength.

Titto said that at GISEC, Accops showcased its product suite. "We have 6 products, but yes, it is called Accops Digital Workspace, along with Zero-Trust network access. These are the two keywords we are selling, which includes complete access to a secure experience, both of the users and endpoints and making sure that customers get access to the right resource at the right time, without any security loopholes. Even data security is extremely critical for us," he added.

Accops is a frontrunner in helping companies transform digitally, and is trusted by a niche clientele. The company has a single integrated solution to take care of remote access, virtualisation, MFA, SSO, DLP & contextual access and provides affordable solutions that come with pre-integrated components, ensuring quicker deployments and substantial cost savings.

"The main concern during the COVID-19 pandemic was that most companies

> "THE MAIN CONCERN DURING THE PANDEMIC WAS THAT MOST COMPANIES WERE UNABLE TO EFFECTIVELY IMPLEMENT REMOTE SECURITY."

were unable to effectively implement remote security and the security of remote connected devices. The immediate solution for this was VPN. But VPN itself is known for its vulnerability, because you are connecting to a network that is vulnerable to any kind of attack. "

So, Accops stepped in to provide comprehensive, zero trust-based end user computing solutions, enabling secure and instant access to business applications to users who work from anywhere, any device and over any network. Accops Digital Workspace suite includes Application & Desktop Virtualization (VDI), Application Access Gateway and Identity & Access Management solutions, helping organisations to swiftly enable work from anywhere within days. Accops is a single-stop shop, taking care of all remote access, application virtualisation, VDI, MFA, identity federation, SSO and client needs. Accops' products are highly modular to fit the needs of businesses of all sizes, providing seamless access to modern web applications, SaaS applications, client-server applications, legacy applications, virtual applications and virtual desktops. 1



GISEC SPOTLIGHT / CYBERKNIGHT TECHNOLOGIES



REINFORCING ZERO TRUST

VIVEK GUPTA, FOUNDER AND COO, CYBERKNIGHT TECHNOLOGIES, ON WHY ZERO TRUST COMPLIANCE IS IMPORTANT FOR COMPLETE SECURITY.

/hat are some of the cybersecurity trends today?

Post the pandemic, what we have seen is that there is an increased threat in terms of both the attacks that are happening, phishing and ransomware in particular, where things have gone to the level of extortion. Also, identity sprawl is something that is becoming very, very prevalent. Therefore, we're all prone to more risks than ever before because of remote working and a lot of people taking a very casual approach to logging in from wherever they have to without ensuring that they are in a secured environment.

Zero Trust security is the buzzword today. Tell us more about it.

Zero Trust is not a very complicated

"WE'RE ALL PRONE TO MORE RISKS THAN EVER BEFORE BECAUSE OF REMOTE WORKING AND PEOPLE TAKING A CASUAL APPROACH TO LOGGING IN FROM WHEREVER THEY ARE WITHOUT ENSURING THAT THEY ARE IN A SECURE FNVIRONMENT." concept. It basically says to always trust but verify. The verification part is very, very important. We look at the five parameters of the Zero Trust security framework when it comes to workloads, people, devices, data and network.

We try and look at all these verticals and create a robust safeguard for our customers so that they are compliant and aware of the risks so that they can safeguard themselves with overall threat perception that they have.

What is your main focus at GISEC?

The vendors that we onboard, the work that we do, is based around the Zero Trust framework. So we propagate this, we get our customers to understand the value of Zero Trust and gradually bring them into compliance, so that they are Zero Trust compliant over a period of time.

ADDING VALUE AT EVERY STEP

JOSE THOMAS MENACHERRY, MANAGING DIRECTOR AT BULWARK TECHNOLOGIES, ON THE COMPANY'S PARTICIPATION AT GISEC AND THE CYBERSECURITY LANDSCAPE POST THE PANDEMIC.

ith an intense focus on boosting the IT security, communications & technology industries in the Middle East region, UAE-based Bulwark Technologies, one of the pioneering IT cybersecurity specialised Value-Added Distributors, showcased an array of internationally acclaimed products at GISEC.

The company reiterated the importance of building a strong, integrated security infrastructure in the region and has also predicted market exigency & introduced apt technologies at the right time.

Bulwark is a cyber security focused VAD operating for more than two decades and GISEC is a great platform for demonstrating our product portfolio to targeted partners and customers in the region. With the region's huge demand for cyber security, we look forward to receiving excellent responses from our vendors, partners & customers during the event," said Jose Thomas Menacherry, Managing Director, Bulwark, speaking to Tahawultech.com. "Value Addition has been at the very core of Bulwark's operations since its inception in 1999, making the company grow from strength to strength. Bulwark today has an established network of over

500 resellers throughout UAE, Saudi Arabia, Qatar, Oman, Bahrain, Kuwait, Jordan, Egypt, Lebanon & other ME countries and the Indian sub-continent region. The company has recently opened their office 'Bulwark Saudi' in Riyadh for providing better services to partners and customers in Saudi Arabia".

"In this connection, we are exhibiting Utimaco – General Purpose HSM or Hardware Security Modules and Payment HSMs, Nexus – the PKI based identity & access management, secure communication for OT and IoT environments, Skurio – Digital Risk

> **"VALUE ADDITION HAS BEEN AT THE VERY CORE OF BULWARK'S OPERATIONS SINCE ITS INCEPTION, MAKING THE COMPANY GROW FROM STRENGTH TO STRENGTH."**

Protection solution consisting of dark web monitoring and brand protection, Help Systems – for Data Security Suite Digital Guardian DLP and Boldon James Data Classification, GoAnyWhere managed file transfer solution, Mimecast - Email Security, Archival, Security Awareness Training, Accops for Thin Client and Remote Secure Access solution, Ekran – Employee Monitoring and Internal Threat monitoring solution, iStorage - Encrypted hard drives and flash drives, adhering to the highest security standards and RiskXchange - for Risk Assessment and Monitoring solution", he said.

About the threat-security landscape today, Menacherry said that the "perimeter" concept vanished when people started working from home. So, it was a tough time for customers and IT teams to give access to employees outside of a network. So, we can say that before the pandemic, although digital transformation had already begun, it accelerated big time during the pandemic and companies had to adopt solutions to keep pace. Now, customers are consolidating all these solutions and streamlining the security landscape itself. But at the same time, we are witnessing a scarcity of skills to handle these solutions as well. 1



PROTECTION ISBETTER THAN A CURE

RAHIL GHAFFAR, DIRECTOR, SALES FOR MIDDLE EAST AND AFRICA AT VIRSEC. ON WHY THE COMPANY IS FOCUSED ON MAKING CYBERTHREATS IRRELEVANT.

ost pandemic, what do you think are the pressing security challenges affecting enterprises?

During the pandemic and post pandemic, there has been a surge of cyberattacks and it's not going to slow down anytime soon especially with the war happening. If you look at the solutions made to counter these attacks, you will find that most of them just 'respond' to these attacks. They are not really protecting against it. So, while, responding and giving visibility is good, what is more important is a solution that can really protect at runtime and not just detect! Because if you just detect, it is giving you the visibility but the damage has already been done and it's "WE PREFER QUALITY OVER QUANTITY AND IN THAT REGARD, WE LOOK FOR FOCUSED PARTNERS SPECIALISED IN CYBERSECURITY AND WHO CAN FOCUS ON OUR PRODUCTS." not protecting an organisation. This is where customers reach out and say that they need an automated solution with almost little to no human intervention and which can protect all the time and not just detect.

We don't want to be seen as someone here to do just business, we prefer to be seen as an entity helping the society and the country to make cyberthreats irrelevant, to detect and prevent them from happening which otherwise gets missed and exists for months together before it is detected as zero day. The industry average is 6.75 days for detecting a new variant. Few vendors also talk about detecting within minutes like 36 to 37 minutes but we talk about detecting and



protecting about milliseconds of the attack happening. This makes a lot of difference for organisations. The IT staff can sleep peacefully at night with the surety that they are protected against known and unknown vulnerabilities deterministically.

Can you tell us about your presence in the Middle East and your partner network?

We have a strong presence in the Middle East especially in UAE and Qatar. We are also expanding in Jordan and KSA and have strong foothold in Africa too. With regards to our partners, we prefer and welcome partners who think like us, who want to make cyberthreats irrelevant for the country and the society because that is what our mission is. We prefer quality over quantity and in that regard, we look for focused partners specialised in cybersecurity and who can focus on our products. We are looking to expand our network with more of these types of partners.

How prepared are partners in helping customers improve their security posture and how is Virsec helping them with the same?

Partners are becoming smarter and gearing up after the pandemic. They devise several ways to support their customers and are doing a good job of the same. They know they must innovate to exist and that is why they are partnering with Virsec since we are the only solution that can protect deterministically across the three layers of the sever, the host, memory, and web close to milliseconds dual time. They are taking our solution to customers who are welcoming it with open arms.

We also ensure that our partners are well equipped in terms of knowledge and skillsets to delight the customers. We help our partners to scale in terms of product knowledge and in providing a smooth deployment of the product. As part of our partner program, they have access to numerous trainings inperson and otherwise, videos, incentive programs, certifications, product updates and discussions that help strengthen our channel and our services to the customer.

LEADING THE MOBILE DEVICE MANAGEMENT MARKET

ROHIT KUMAR, SALES HEAD-APAC & ME, 42GEARS MOBILITY SYSTEMS, ON THEIR PARTNERSHIP WITH BULWARK AND THE TECHNOLOGIES SHOWCASED AT GISEC.

ell us about 42Gears' partnership with Bulwark.

42Gears has a solid partnership with Bulwark. We began our engagement around 4 years ago. We have our headquarters in India, we have offices in the US and the UK, but as a part of market strategy, we focus on localisation and key partnerships. I take care of the APAC region. So as a part of the strategy, we have a localisation which we do with our partners. Having said that, we have a very wide and growing market. We see a lot of potential in the region and that is why we wanted to be associated with one of the leading distributors and partners who can take care of the local market requirements, technical analysis, POCs, demos and all other aspects.

"WE SEE A LOT OF POTENTIAL IN THE REGION AND THAT IS WHY WE WANTED TO BE ASSOCIATED WITH A LEADING DISTRIBUTOR LIKE BULWARK." From their we connected with Bulwark where we are getting huge support. They have expertise in the product. They are extensively connected in the same industry. They have other partners who are working very well in the same technology. So, this has given us a good visibility in this market. And today we are having a very good mature business working with Bulwark.

Are you showcasing any technology solutions at GISEC?

We are a product-based company and we have our own product which is very much into mobile device management. And we have been an expert and industry leader when it comes to company-owned devices. We have huge deployments globally and the technology we are into is key for many industries in this region.

We have important customers here who are using our product to minimise the misuse of the devices. So, that is the technology which bring which we bring in to ensure device protection. There are also so many other related features that we provide with our product.

How important is this market for you?

The Middle East market is extremely important-most of the decisions from EMEA come from Dubai. We have been participating in GISEC and GITEX for a few years now and we have seen very enthusiastic response from companies in the country and the region. So sitting in Dubai, we are able to access all the major markets and we are looking to expand our footprint in this region. We see very good market growth here and there is lots of potential. Now, we are able to make good investments for a better ROI. So yes, this market is very, very important in our growth plans. **1**



DEFENDING CRITICAL INFORMATION OF THE SECURITY

STRATEGIST AT TENABLE, ON THE DIFFERENT TYPES OF CYBERSECURITY THREATS FACED BY ORGANISATIONS POST THE PANDEMIC .

Fast paced digital transformation has bought about its own security risks. At present, we mostly see three main threats. Number

one is due to remote working. We all know that remote workers are here to stay. Companies won't go back to operating the way they did two years ago, before the pandemic. Certainly, people are willing to go back to office but the fact that some of them still opt to work remotely, will continue to be a threat because the home network is not secure. A home network has plenty of devices, roughly about eight devices connected at a time which includes corporate devices as well and this a vulnerability that can be easily targeted by attackers," Montel said.

"The second is attack against critical infrastructure. In Europe, Middle East, and Africa, they are the main targets for cyber criminals and the trend is very high. Almost 45 percent of attacks are ransomware attacks which is the top threat right now against critical infrastructure. Third is due to cloud adoption. Because of the surplus amount of people working from home, we needed to launch new cloud services to ensure continuity and we had to do this in a couple of weeks. Now cloud adoption is something we have been talking about for the past 10 years but rapid cloud adoption was brought about by the pandemic and we have attackers who are now willing to target

the cloud provider rather than targeting a particular company. Why so? Because if they target a cloud provider, they can hit hundreds of companies so the effort is the same but it will have a domino effect that will affect hundreds of companies at a time."

Montel went on to talk about how critical infrastructures like healthcare are easy targets for attackers looking to make quick monetary benefits, "In EMEA, the top three sectors are education, government and healthcare. Of these, healthcare is the number one sector which is vulnerable to attacks. Hospitals have not been designed to beat cyber security threats. Their main mission has always been to save people. During the COVID-19



pandemic, they were under fire to save people's lives leaving them vulnerable to cyber-attacks. We must bear in mind that the nature of healthcare data is unique. If you have a data breach for intellectual property, the data can have a new version, it can be changed and hence it won't be sensitive data anymore. Same goes for financial data. However, in the case of data related to human beings, the data will always be unique. For example, you cannot change your disease, your date of birth or your social security number. You can't have a version 2 of the history of your diseases! So, when this type of data is out, it is considered highly sensitive and because of that its highly monetised by attackers. About 98

"MY ADVICE TO COMPANIES LOOKING TO IMPROVE THEIR CYBERSECURITY POSTURE IS TO PRIORITISE. "

percent of the attacks are ransomware attacks and the majority of any sort of attack focuses on vulnerabilities. They penetrate the network using these vulnerabilities which have been there for many years because hospitals, have not been designed for cybersecurity but for saving lives. They use technology mainly for medical purposes and thus are prone to be easy targets for an attack."

"My advice to companies looking to improve their cybersecurity posture is to prioritise. There are hundreds of vulnerabilities that come up every day. You cannot patch up all of them. There should be an approach based on risk. If we are to talk about business risk, we must consider which are the technologies that are business critical be it on-prem or on cloud; if there are any vulnerabilities, this is where the effort must go for patching. Also keep in mind specific software's that might have access to active directory and admin rights. These are very sensitive and must be taken care of. Another step is detecting vulnerabilities in cloud applications. When we move to the cloud, we move to native cloud applications that are designed and coded directly with containers and Kubernetes and that type of technology. If we fail to check for vulnerabilities in the code when the applications are being developed, it will be too late. We must thus shift left and detect vulnerabilities in the code itself which will ensure huge benefits later," Montel added. 1

REDEFINING OT SECURITY

BACHIR MOUSSA - REGIONAL DIRECTOR, MEAR AT NOZOMI NETWORKS, SPOKE TO SECURITY ADVISOR ABOUT THE DEMAND FOR OT/IOT SECURITY SOLUTIONS IN THE REGION.

hat products and solutions did Nozomi Networks showcase at GISEC 2022?

OT and IoT Security is our forte and so this GISEC we highlighted how to gain real time visibility in a passive manner into your OT and IoT environments, and how to build on that visibility to leverage cybersecurity that helps protect and detect cyber threats early on before they impact the environment. We also demonstrated management of your OT and IoT environment from a security perspective, whether it is on premise or cloud, with our vantage platform.

Post pandemic, what do you think are the pressing security challenges faced by companies?

Post pandemic, we know that many people do not prefer to go back to working onsite and so remote access continues to be a very important part of day-to-day work. This is where we step in, for remote access to the industrial network. This is very critical because if done well, it saves a lot of time and allows organisations to work efficiently – even remotely. However, if not done well, it exposes the industrial network and induces a lot of threats, and a threat in an industrial network could mean a threat to the general population – that being us. Take for example, a utility organisation's remote access. If there is a threat, then the station can go down, impacting the availability of electricity and water to the general population. Therefore, remote access continues to be a very important vulnerability to be dealt with.

How has COVID-19 impacted the thought process around OT/IoT security?

The pandemic has made cybersecurity more prevalent. Post pandemic, it has now also become more important in the minds of operational technology leaders. Now we see more interest from their side in what we provide in the form of security and visibility. Organisations know that they have to be ready now and for the future because they must react quickly incase the need arises. It has also woken up government



organisations. We have seen a lot of compliance and regulations coming from government regulators in the Middle East, as well as globally from USA and Europe.

How would you describe the demand for OT and IoT security solutions in the UAE and what are your plans and strategy for the Middle East?

Events such as GISEC that show the interest of the UAE Government with regards to cybersecurity, help raise awareness among organisations. We see the demand grow significantly because of this awareness and because of the compliance and regulations that are pushing organisations to take action. As Nozomi Networks, we have been WE HAVE BEEN FOCUSED ON THE UAE FROM A VERY EARLY STAGE AND HAVE GROWN EXPONENTIALLY OVER THE LAST FEW YEARS. focused on the UAE from a very early stage and have grown exponentially over the last few years. We believe in providing the right products and the right support on ground for our partners and customers alike. Our focus and strategy are to keep growing in the Middle East by continuously providing this support and by hiring more skilled personnel.

In the last one year we have grown from 60 to 70 percent with regards to personnel, and we want to keep investing here because the region is large and complex, and we believe in local support rather than flying people down to provide support. We also have a large partner network focused on cybersecurity and partners that focus on industrial networks. **1**



FOCUSED ON INNOVATION

SULTAN AL-HARBI, OT SOC MANAGER AT IT BELT, SPOKE TO SECURITY ADVISOR ABOUT THE COMPANY'S INNOVATION-FIRST STRATEGY AND PLANS FOR THE REGION.

T Belt is a Saudi company that was established in 2008. It specialises in IT/OT cyber security, IT infrastructure, loT, and physical security solutions and services provider in KSA and GCC region. Headquartered in Riyadh, ITB provides world-class services and solutions combined with strategic consulting across multiple sectors enabling them to build and protect their businesses.

"Our vision is to provide world-class, innovative, value-added services, and guidance to our customers while establishing a regional and worldwide position of leadership," Sultan Al-Harbi said. "This is underscored by our mission to provide a state-of-the-art IT solution to our customers and to differentiate ourselves with a professional project management that will improve the level of performance, as well as increase the success rate of projects and achieve the project objectives."

The company provides vital, cutting-edge cybersecurity services and solutions that cater to the latest "OUR VISION IS TO PROVIDE WORLD-CLASS, INNOVATIVE, VALUE-ADDED SERVICES AND GUIDANCE TO OUR CUSTOMERS WHILE ESTABLISHING A REGIONAL & WORLDWIDE POSITION OF LEADERSHIP." market trends. "As digitalisation continues to prose its risks on privacy and security, it has become absolutely crucial to protect the lifecycle of your business and secure it properly. By identifying network vulnerabilities, we establish an effective cyber resiliency strategy that harnesses all of our expertise and latest technologies against deliberate attacks, malware and security breaches," Sultan Al-Harbi said.

The company has innovation and excellence at the core of all its activities. "ITB with its partners possess a large database of customers in the Saudi Arabia and GCC with the same engagement required by client references. As a specialised company in IT Infrastructure and Security Solutions and Services, the top management aspiration is all about developing outstanding solutions & services for clients. Our talents are well employed for our clients. Our reputation and record of accomplishment proves it all," Sultan Al-Harbi said. 🚺

EVERY DAY SHOULD BE WORLD BACKUP DAY CLAUDE SCHUCK. REGIONAL DIRECTOR MIDDLE EAST. AT VEEAM SOFTWARE

XO research from Veeam has found that 86% of EMEA organisations have a protection gap between how much data they can afford to lose and how often IT systems are protected. This has risen by 14% in the past 12 months and indicates that while the criticality of data continues to soar, so do the challenges in protecting data to a satisfactory level. World Backup Day 2022, that was observed on March 31, is another reminder that as both the cyber threat landscape and IT environment complexity continue to increase, the need for robust data protection measures is more vital than ever. A solid backup, replication, and recovery plan is a key component of any Modern Data Protection strategy that ensures business continuity and the capacity to take immediate action.

Why backup matters

Almost every organisation experiences unexpected outages, according to the Veeam Data Protection Trends Report 2022. There are many incidents that can lead to downtime. Among EMEA businesses, these are commonly caused by infrastructure or networking outages, server hardware failures, and application software faults. Furthermore, ransomware and other cyber threats are compounding the situation – with 51% of EMEA organisations suffering outages at the hands of a cyber-attack in the past 12 months.

Backup best practice: Simply put, any data that is not backed up can be lost forever in the event of an outage. While the threat landscape is daunting, the general rule of thumb for a robust Modern Data Protection strategy are consistent. No matter how data is compromised, whether hardware and power failure, accidental deletion, or cyber-attack, if it has been protected in line with Veeam's 3-2-1-1-0 backup rule. you can get it back. There should always be at least three copies of important data, on at least two different types of media, at least one off-site and one as immutable copy offline, and finally, with zero unverified backups or backups completing with errors.

"WHILE THE THREAT LANDSCAPE IS DAUNTING, THE GENERAL RULE OF THUMB FOR A ROBUST MODERN DATA PROTECTION STRATEGY ARE CONSISTENT."

Ransomware is a new norm

There is still a perception that ransomware strikes an unlucky few, but this is not the case. The majority (71%) of EMEA organisations have suffered ransomware attacks in the past 12 months. Given the inevitable nature of cyber-attacks like ransomware, it's paramount that businesses can recover. However, according to Veeam's survey respondents, over one in three (36%) organisations are unable to recover data after a ransomware attack. Therefore, we now have the situation that it is no longer a question of whether businesses are experiencing ransomware incidents, but rather when. There are still far too many organisations that are unable to recover the data they lose.

Cybersecurity best practice: There are three elements that create the ultimate strategy to protect data against ransomware. The first line of defence is using education to build a human firewall. Prepare your employees with the digital hygiene tools and knowledge needed so that they do not fall for some of the oldest tricks in the cybercrime book like phishing. Make sure this is an integral part of your business practices. The second is implementation. Implement the 3-2-1-1-0 backup rule; invest in solid Disaster Recovery provisions in accordance with your defined RPOs and RTOs; ensure you've protected data across all platforms

including physical, virtual, cloud, SaaS, and Kubernetes. Finally, it's remediation. If your education and implementation strategies fail, do not pay the ransom. The only option is to restore data.

Future-proof your data protection investment

The ability to move workloads from one platform to another – including physical, virtual, and cloud-hosted – enables organisations to progress with Digital Transformation initiatives and retire legacy backup tools. But not at the expense of IT resilience. Veeam enables both cloud-powered data protection, as well as protection of cloud-hosted workloads such as SaaS and containers, with full backup and recovery, disaster recovery, application mobility, and ransomware protection. It is essential for decision-makers to understand that data is the lifeblood of their business and investment in Modern Data Protection is an investment in their future. 1

INSIGHT / HIKVISION



etting clear views over a large area – such as a major traffic intersection, a warehouse, or a parking lot – isn't always a simple task. It typically calls for multiple cameras and extensive

for multiple cameras and extensive cabling to be installed at a variety of locations, in order to cover the entire field of view.

But when it comes to installing hardware, the requirements can differ widely from one scenario to the next.

At Hikvision, we take these requirements and so much more into account. Our range of security solutions not only help customers increase their on-site security with complete coverage, but add value with components that simplify their day-to-day security and business operations. These include Hikvision's PanoVu Series Panoramic Cameras, Ultra Series PTZ Cameras, and Fisheye Cameras, as well as the newly released line of TandemVu PTZ Cameras.

Flawless panoramas with extraordinary imaging

In large open sites like sport stadiums, plazas, and intersections, common security challenges are often about the large security scale, which requires several cameras to cover all corners of the view. This results in increased costs and difficulties in deployment. On the

> IN LARGE OPEN SITES LIKE SPORTS STADIUMS, PLAZAS AND INTERSECTIONS, COMMON SECURITY CHALLENGES ARE OFTEN ABOUT THE LARGE SECURITY SCALE, WHICH REQUIRES SEVERAL CAMERAS TO COVER ALL CORNERS OF THE VIEW.

other hand, a large scene also indicates a need for HD images, so that security operators can enlarge the imaging to see details.

Thanks to the company's advanced image stitching technology, PanoVus stitch images together to generate a single, seamless panoramic picture with 180° or 360° coverage, allowing security operators to enjoy a vivid and consistent viewing experience that's more true-to-life.

Pan, tilt, and zoom at any moment

In some cases, security coverage in critical areas becomes primary. When events happen, it is important to view the close-ups with high-definition detail.

One advantage of PTZ cameras is their automatic patrolling capability. That means security operators can set rules for the cameras to monitor needed areas with defined duration, frequency and timing, to name a few. Additionally, Hikvision's Ultra-Series PTZ Cameras feature ultra-high optical zoom - 42x, for example – to cover expansive areas. That



allows security operators to zoom in on an object which is farther away, ensuring clarity in the details.

The Ultra Series cameras' night vision capability is also stunning, as they incorporate Hikvision's signature DarkFighter low-light technology which enables excellent HD images to be captured in light conditions down to 0.0005 Lux.

Big picture and small details in one view

There are also situations where a security view with wide-angle coverage needs to be maintained at all times, yet close-ups are needed for awareness if an incident occurs. An example can be a busy outdoor parking lot at a shopping mall.

By using Hikvision's new TandemVu PTZ cameras, facility managers can now maintain focus on both "viewpoints" simultaneously – monitoring large areas for overall situational awareness and zooming in on specific incidents for event management.

When smaller areas need complete coverage

In places with less space to cover, such as retail stores and meeting rooms, complete coverage with situational awareness is often the first security priority. Therefore, a vertically-oriented view from the ceiling to the floor provides better coverage of a whole area. Fisheye cameras play their best roles here.

Hikvision Fisheye Cameras are among the most sophisticated on the market today. Featuring top-of-therange Immervision lenses, they deliver a wider angle of view, less distortion, and sharper, more detailed images than many other cameras on the market, which results in more natural images once they have been dewarped.

Incorporated with deep-learning-based AI applications such as heat mapping, intersection flow analysis, and people counting, Hikvision fisheye cameras empower users with a wealth of data for business analysis, reporting, and smarter decision-making.

Efficient centralisation

All these devices and technologies need to be managed, and this is where a powerful VMS like Hikvision's HikCentral Professional comes in. Security operators can view real-time information via HikCentral Professional video management software, cruise around in panoramas, or zoom in and out.

Secure more with more assurance

Hikvision strives to help professionals from many walks of life stay confident and assured with future-shaping technologies, just as our advanced cameras address security challenges in protecting large sites and open areas. Apply for a smart trial today for a handson experience with Hikvision's highperformance products – now guaranteed with a 5-year warranty! Also visit our website to learn more. You can further explore the Hikvision digital showroom for complete Hikvision product lines, core technologies, scenario-based solution packages and more. **1**

INTERVIEW / AXIS COMMUNICATIONS

SMARTER, SAFER

xis Communications, a global leader in security and surveillance solutions offers products and services for video surveillance and analytics, access control, as well as intercom and audio systems. As the industry leader in network solutions that enable a smarter and safer world, they were part of Expo Dubai 2020 as an official partner of the Swedish Pavilion at the expo's sustainability District where they showcased their intelligent security solutions for smart cities.

Axis hosted six transformative technology conferences at Expo Dubai 2020 from 1 October 2021 to 31 March 2022. The final conference, under the theme of, 'Share in the discovery of cybersecurity', wasinsightful and focused on security best practices.

Steven Kenny, Architect & Engineering Program Manager, EMEA, Axis Communications and one of the speakers at the event sat with our contributing Editor Nitya Ravi to talk about security trends, best practices, and the like.

Tell us about Axis Communications and its part in Expo 2020.

Axis Communications is a Swedish

organisation that enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. We partnered with the Swedish pavilion this Expo 2020 to demonstrate the technologies that we are providing across the market. We held six events during the Expo which focused on different trends we see across the marketplace, including AI, Sustainability, Cybersecurity, 5G.

What do you think is the impact of cybersecurity on physical security systems?

There is a massive impact. The way physical systems have been deployed today has fundamentally changed from what it was ten to fifteen years ago. These are systems that provide security functions, so we need to consider how we embed cybersecurity in them, how they are deployed and how they are managed and maintained because a physical security system is a huge risk to an organisation if they don't consider the cybersecurity aspect as they do with all their IT systems. A potential attacker would always choose to follow a path of least resistance. They don't care what

they attack whether it's an access control door, whether it's a video surveillance camera or a laptop or phone. So physical security systems should absolutely follow all the other IT policies that businesses have in place.

How do you think has been the awareness with regards to the importance of physical security and the need to converge it with IT security post pandemic?

The concept of convergence has been discussed for many years. There has been a great level of awareness around the impact of cybersecurity on physical systems post pandemic because the pandemic essentially created a huge number of vacant properties. For businesses to monitor the security of these systems, they had to change the way they were operated a lot of these systems had to essentially open themselves up to third parties, remote monitoring sensors etc that can monitor them because there was no one on these sites anymore. Hence, companies are more aware of the exposure to opening these systems which is one of the very few positives to potentially comes out of such a tragic period.

What do you think are the current cybersecurity trends and best practices?

There have been top 5 cybersecurity trends identified for 2022.

Al Power cybersecurity: This is one of the growing trends we see for cybersecurity. It is a double-edged sword as in it can be used for good and bad. We see that businesses adopt Al type applications to support their cybersecurity strategy but so do the criminals. The criminals use these same systems to identify vulnerable applications and to compromise or manipulate databases.

Ransomware - Ransomware has shot through the roof during the pandemic to the extent that governments have put out guidance for businesses on how to make their employees more aware about the consequences of clicking an email when they do not know where and from whom it has come from. Social engineering attacks happen daily, and organisations are crippled because their ability to carry out business would come to a halt when important business files are encrypted and can't be accessed whether it be customer data, accounting data or information around their own technologies. They say this is the proverbial get rich quick scheme for criminals. To do some form of ransomware, all that the attackers need is a low entry PC and anybody and everybody who wants to get involved can do it.

IOT vulnerabilities – There are tens of thousands of IOT devices that are being pushed to the market and these devices have vulnerabilities when they are released. The truth about these devices is that organisations only take revenue from the product when it's sold in the market and vulnerabilities are discovered once they are in the market. Companies must then back pedal once a security issue has been identified.

Supply chain attack – This happens

"TO IMPROVE YOUR CURRENT SECURITY POSTURE IS TO MAKE EVERYONE AWARE IN YOUR ORGANISATION THAT THEY ALL HAVE THEIR PART TO PLAY IN THE ORGANISATION'S SECURITY REGARDLESS OF THEIR ROLE, THEIR FUNCTIONS, OR RESPONSIBILITIES."

when organisations are attacked not because the bad actors want to attack that organisation but because of who that organisation is working for or that organisation is providing technology to. So, supply chain attacks are huge in that regards.

Regulation changes – We are starting to see different countries starting to enforce legislation, that they are starting to create regulations, or even just cyber security certification. Governments are starting to make a positive change and influence the cybersecurity considerations.

How can companies futureproof their assets?

To future proof your assets, there must be a cultural and mindset change. Businesses need to revaluate the way they procure technologies. Businesses tend to start with how much does a technology cost and then they look at their operational costs and try to see whether there is an alignment. All they need to do is change that and give a bit more due diligence to considerations like what is the impact of the technology on my business, do I have strong IT policies and procedure, can I demonstrate cybersecurity maturity etc - that is where business should start because that doesn't cost anything other than time.

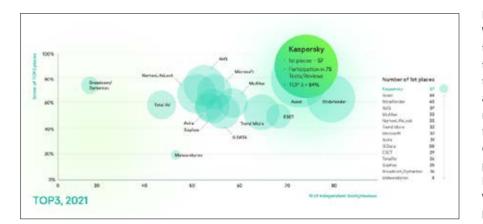
Once businesses get that part right, it will safeguard their future investments and they can start to evaluate how these systems can be used in different ways. For example, if we were to look at it from a physical security perspective, when you know you have a secure technology then you can start connecting it to other third party systems because you are not putting those systems at risk and you can also use it for business optimisation and to look at new intelligent initiatives from the same piece of technology. That is the quickest and easiest way to safeguard the investment you made.

What advice would you give to companies looking to improve their current security posture?

To improve your current security posture is to make everyone aware in your organisation that they all have their part to play in the organisation's security regardless of their role, their functions, or responsibilities. When businesses talk security, it must be implied that everyone in that organisation can impact the security posture of that business especially from a cybersecurity point of view.

How can companies do that? They can provide education, make people aware of consequences of the decisions that they make by clicking on an email or putting an USB stick into a computer. We are not asking companies to buy a technology or redesign the way they do their business; we are just asking them to embrace an education program to make their people aware that they have a part to play and in this way they can go a long way in ensuring a stable security posture. **1**

KASPERSKY TAKES TOP SPOT IN 76% OF TESTS, DEMONSTRATING TECHNOLOGICAL EXCELLENCE



n 2021, Kaspersky's security portfolio held the leading position in the TOP3 metric. Over the year, Kaspersky participated in 75 independent tests and reviews with its products being awarded 57 firsts and 63 TOP3 finishes.

The TOP3 metric shows how successful a vendor is by measuring its performance across a number of independent tests within a calendar year. Consistent performance across multiple tests and products gives a more meaningful assessment of the company than the results of a single test. The TOP3 metric includes results from lab tests, such as AV-Comparatives, AV-TEST, SE Labs and others.

Among the numerous tests considered in 2021's TOP3, some are particularly noteworthy. The 'Advanced Endpoint Protection: Ransomware Protection' test performed by AV-TEST, saw Kaspersky Endpoint Security Cloud achieve the highest possible result, protecting against all ransomware attacks used in the research. SE Labs awarded Kaspersky Endpoint Detection and Response with the highest-grade. 'AAA.' in the Enterprise Advanced Security (EDR) Test because the product detected every one of the 16 targeted attacks from 4 groups with no false positives and a total accuracy rating of 98%. Kaspersky Endpoint Security for Business received the 'Advanced' award from AV-TEST in the Advanced Threat Protection Test against ransomware and was also granted several other annual awards from the organization, including 'Best Protection', 'Best Performance' and 'Best Usability.' Kaspersky Endpoint Security for Business has also been ranked by IDC as a Major Player in the IDC MarketScape and was noted for its ability to offer enterprise customers a natively integrated cross-product solution.

As for consumer solutions, Kaspersky Internet Security has been highlighted in several annual awards, such as 'Best Protection and Best Performance' by AV-TEST. AV-Comparatives also ranked Kaspersky Internet Security as 'Top Rated' in 2021 with four specific area awards: ATP 'Advanced Threat Protection' 2021 Silver, 'Best Overall Speed' 2021 Silver, 'Lowest

False Positives' 2021 Silver and 'Real-World Protection' 2021 Silver. On top of this, Kaspersky Internet Security received the 'Advanced' award from AV-TEST in the Advanced Threat Protection Test against ransomware, Kaspersky Safe Kids received AV-TEST's 'Approved' recognition for a comprehensive split of features that ensure sweeping protection across all platforms (Windows, Android and iOS). In addition, AV-TEST named Kaspersky VPN Secure Connection as one of the best solutions for gaming and streaming, highlighting its solid speed ratings and its strong transparency offerings for the user. SE Labs has also highlighted Kaspersky Internet Security and ranked it with the highest grade, 'AAA,' with the product achieving the highest total accuracy rating at 100% in Q2 and Q4.

Additionally, between the years 2013 and 2021, Kaspersky products participated in 741 independent tests and reviews within the TOP3 Metric. Over this period, Kaspersky solutions were awarded 518 firsts and achieved 612 top-three finishes.

"Continual participation in independent tests is an integral part of the effective development of technologies, which can then be efficiently incorporated into cybersecurity solutions. Regular analysis of such results allows us to discover real areas for improvement in our technology and confirms the levels of protection provided to our customers from real cyberthreats. We are pleased to have received such high results in 2021, which once again demonstrate the high quality of our security technologies and solutions," said Alexander Liskin, Head of Threat Research at Kaspersky. **1**



solarwinds SECURE BYDESIGN Leading the Way to Safer IT

Secure by Design guides our delivery of powerful, affordable, and secure solutions. We're confident our actions will create the most secure and high-quality software in the industry.



L'nksys^{*}



Model# MX5500 MX5501

Atlas Pro 6

Whole Home Mesh WiFi 6 Dual-Band System

Powered by



Velop Intelligent Mesh. New Launch

Covers homes with up to

4-5 bedrooms | 90+ Devices | AX5400 up to 5.4 Gbps

A better WiFi has arrived

Simultaneous video calls, gaming and high-speed data capacity

Key Features

WiFi 6 Offers 4x More Capacity*

Mesh WiFi 6 delivers true gigabit speeds—up to 5.4 Gbps with 6-stream connectivity—throughout your entire home inside & out.

160 MHz Capable

Access to 160 MHz channels—the least congested on the 5GHz band—unleashes WiFi 6's incredibly fast connectivity, allowing work-from-home, online learning, streaming & gaming devices to operate simultaneously without reduced bandwidth.

More WiFi Channels

Dynamic Frequency Selection (DFS) reduces interference from neighboring networks.

Industry-Leading Technology

The Qualcomm[™] Immersive Home 216 Platform transforms home & business WiFi to wired-like stability and speed.

Easy Setup and Control

It's simple to set up and lets you manage your network or prioritise devices from anywhere, all with the free Linksys app.



Easily Control your Network, Anytime, from Anywhere

Multi-site cloud managed Wireless Access Points purpose built for business networks.

IN-WALL 1300AC WiFi 5 MU-MIMO Cloud Managed Wireless Access Point LAPAC1300CW Outdoor 1300AC WiFi 5 MU-MIMO Cloud Managed Wireless Access Point LAPAC1300CE

- Dual-Band 802.11AC Wave 2 MU-MIMO (2.4GHz + 5GHz)
- 3 Gigabit Ethernet Ports
- 802.3af PoE and 802.3at PoE+ Compliant
- 802.3af PoE Passthrough (requires 802.3at PoE+ Input)
- Two-Factor Authentication for Cloud Account Login
- Reduce time on-site with Zero Touch Provisioning
- Limited Lifetime Cloud Management

- Dual-Band 802.11AC Wave 2 MU-MIMO (2.4GHz + 5GHz)
- 2x2:2 for AC1300 Speeds (400Mbps + 867Mbps)
- Four (4) Removable Antennas (SMA)
- IP67 Rated for Outdoor Applications
- 802.3af/at PoE or PoE+ Support
- Limited Lifetime Cloud Management
- TAA Compliant