WWW.TAHAWULTECH.COM

ADVISOR

WHY Password Hygiene Matters

CYBERKNIGHT ACCELERATES INTELLIGENCE-LED SECURITY

WINNING THE CYBER BATTLE:

WHY IT'S TIME TO RE-IMAGINE THE SECURITY STACK

MIDDLE EAST

0

SPECTRAMI'S ANAND CHOUDHA

D

SAART VIDEO SURVEILLANCE SOLUTIONS ARE DELIVERING BENEFITS

BEYOND SECURITY

computer news middle east SUPPLEMENT

🛞 tahawultech.com

ClickShare

Conference, Collaborate, Click!

Discover the new ClickShare Conference

Let the new ClickShare Conference transform your remote meetings. Gone are the frictions when you host a conference from your laptop, or the struggle trying to use cameras and other meeting room equipment. Simply launch the ClickShare Collaboration App or plug in the ClickShare Wireless Conferencing Button. In less than 7 seconds you are ready to go.

BARCO

CONTENTS

14 Smart vision

Hyvision Technology's Leo Liao on how smart video technologies are delivering value beyond security

۲



Securaty







12 WHY PASSWORD HYGIENE MATTERS

Sophos' Paul Ducklin on why it's time to rethink approaches toward password change



22 A CLEAR VIEW Hikvision shares why smart

video solutions are vital in maintaining social distancing

30 WINNING THE CYBER BATTLE

Fidelis' Rawad Darwich on why it's time to re-imagine the security stack

34 DEFENDING THE HUMAN FACTOR

Why UAE enterprises need a people-centric approach in defending their workforce



NEXT GENERATION FIREWALL

With all-new Data Security Approach and Contextual Intelligence Engine for security beyond just the perimeter.

FEATURES



GAJSHIELD

GAJSHIELD

GS160n

https://me.dlink.com/

D-Link[®]



EDITORIAL



Talk to us: E-mail: adelle.geronimo@ cpimediagroup.com

Adelle Geronimo Editor

EVENTS



ONE STEP AT A TIME

When COVID-19 was declared as a pandemic

a few months ago, it caused tremendous disruptions to economies across the globe. The restrictions set in place by governments have pushed many businesses to adopt remote working schemes and to reduce their operations while some have been forced to shut down completely.

This unprecedented reality has also sprung a new wave of cybersecurity challenges for organisations as threat actors "79% OF take advantage of the fear and **ORGANISATIONS** uncertainties caused by the SAID THEIR pandemic. MAIN PRIORITY **IS TIGHTENING**

As the landscape shifts, businesses must evolve their strategies too and re-think the security measures they set in place. A study conducted by CheckPoint

Software Technologies revealed that 79 percent of organisations said their main priority is tightening security and preventing attacks as they ease into the 'new normal.'

However, what's promising is the commitment of technology players to developing new tools and solutions to both help protect individuals against the virus and secure organisations against cyber-attacks.

On the front cover of this month's Security Advisor ME, we spoke to Hyvision Technology general manager Leo Liao who discussed how the company is helping businesses to stem the outbreak through its range of innovative security solutions. Liao also highlighted how the smart surveillance market has evolved to deliver benefits that go beyond security

> and discussed the company's strong partnership with Seagate.

It also features a one-to-one discussion with Avaya's Sumedh Ganpate who elaborated on how the company developed Avaya Spaces with security at the core. He also elaborated on the platform's latest security feature called 'Private

Space' and touted how Avaya is continuously innovating to ensure that Avaya Spaces remains reliable and secure.

This edition of Security Advisor ME also contains top insights from Spectrami, Hikvision, Fidelis and more. Happy reading!

Published by

CPI MEDIA GROUP

C P I M E D I A G R O U P. C O M

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com +971 4 440 9139

ADVERTISING Group Sales Director Kausar Syed kausar.syed@cpimediagroup.com +971 4 440 9130

FOUNDER, CPI MEDIA GROUP

Dominic De Sousa (1959-2015)

Senior Sales Manager Sabita Miranda sabita.miranda@cpimediagroup.com +971 4 440 9128

EDITORIAL Online Editor Adelle Geronimo adelle.geronimo@cpimediagroup.com +9714 440 9135

Contributing Editor Mark Forker mark.forker@cpimediagroup.com +9714 440 9153

DESIGN Senior Designer Analou Balbero analou.balbero@cpimediagroup.com +971 4 440 9140

DIGITAL SERVICES Web Developer Jefferson de Jova

+971 4 440 9100

Registered at Dubai Production City, DCCA PO Box 13700 Dubai, UAE

> Tel: +971 4 440 9100 Fax: +971 4 447 2409

Printed by Emirates Printing Press LLC, Dubai

> © Copyright 2020 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.

webmaster@cpimediagroup.com

SECURITY AND

PREVENTING

ATTACKS"

ABU DHABI-BASED INJAZAT UNVEILS NEW CYBER DEFENCE FACILITY

UAE-based digital transformation leader Injazat has unveiled its new Cyber Fusion Centre, expanding its cyber defence capabilities and portfolio of services.

According to Injazat, the new facility is a first-of-its-kind in the region and will provide, Abu Dhabi's Mubadala and its group of companies, protection against data breaches and cyber-attacks.

Injazat's Cyber Fusion Centre has been designed to approach security in a holistic manner and to evolve beyond the conventional 'monitor and respond' model of most security operations centres. By embodying elements such as threat detection and response, in addition to intelligence sharing and analysis, the centre empowers businesses to gain a holistic overview of cybersecurity processes, in order to operate with greater awareness and efficiency.

Cyber Fusion Centre leverages artificial intelligence, machine learning and behavior analytics to provide a proactive and unified approach to neutralise potential threats. Injazat has

also added additional highly skilled security analysts and engineers to its existing talent



pool, to further boost operations within the Cyber Fusion Centre.

"Injazat has a long history of successfully supporting the critical and highly visible entities of the Abu Dhabi Government. Now we are taking our experience and knowledge to develop and deploy next-generation cyber capabilities and solutions for the region and beyond," said Khaled Al Melhi, CEO, Injazat.

The first phase of the project saw a number of leading companies onboarded onto the Cyber Fusion Centre with an additional group of eight companies scheduled to begin receiving services within 2020. "With the launch of the Cyber Fusion Centre, we are bringing our customers" IT security operations under one roof, thereby providing a holistic overview of processes for increased efficiency and awareness," said Al Melhi.

Injazat is leveraging its successful track record of supporting business critical services. The company is applying the knowledge and expertise it has built up to develop and deploy next-generation cyber capabilities and solutions.

Once the second phase by the Centre is completed, Injazat will then expand its services to the wider UAE market within the third quarter of 2020.

EMEA LEADS IN MULTI-CLOUD ADOPTION, SECURITY CHALLENGES REMAIN: F5

EMEA region leads the way for multi-

cloud adoption, although security and skill gap challenges remain, according to the latest figures from F5.

According to the sixth annual State of Application Services (SOAS) report, 88 percent of EMEA firms are now leveraging multi-cloud environments, compared to 87 percent in the Americas and 86 percent in the APCJ region, according to the sixth annual State of Application Services (SOAS) report.

It also highlighted that 27 percent of EMEA respondents also claimed they will have more than half of their applications in the cloud by the end of 2020. Meanwhile, 54 percent agree that cloud in all its forms is the top strategic trend for the next two to five years.

However, 33 percent of EMEA organisations cite regulatory compliance as the biggest challenge when managing applications in multi-cloud environments, which is once again higher than any other region, and partly due to complexities stemming from the EU GDPR.

Other pressing concerns include applying consistent security policies across all applications (30 percent), safeguarding against emerging threats (28 percent), and migrating applications between clouds and data centres (28 percent).

When it comes to security postures, respondents reported lower confidence levels in their ability to withstand an application-layer attack in the public cloud (only 15 percent were "very confident" they could do so), versus in an on-premises data center (30 percent) or via colocation deployments (20 percent).

The cloud security challenge is further exacerbated by a growing industry skill gap: as many as 66 percent of EMEA organisations believe they lack necessary security talent going forward, according to the study.

Despite EMEA's proactive embrace of per-app cloud strategies, the SOAS report found that many still struggle to provide security parity across all application environments.

US-BASED POWERDMARC SIGNS ON DISTI360 AS REGIONAL DISTRIBUTOR



ABDULLAH ABU-HEJLEH, DISTI360

US-based email authentication

solutions provider PowerDMARC has announced that it signed a distribution agreement with Dubai-based Disti360.

Under the new partnership, Disti360 will distribute PowerDMARC's suite of email security and DMARC services across Saudi Arabia, UAE, Kuwait, Bahrain, Jordan and Egypt.

Disti360 will be PowerDMARC's

first major distributor in the Middle East. With many new businesses and organisations forming all around the region, there's a growing need for a proper solution that protects against malicious phishing scams.

"We're excited to be among the first ones to offer fully-featured email security services to businesses in our region," said Abdullah Abu-Hejleh, Founder & CEO of Disti360. "It's a rare opportunity for us and our partners. Together with PowerDMARC, we can forge strong connections with organisations all across the Middle East, securing domains and making email and cyber safer for everyone."

CYBERKNIGHT BRINGS CLEARSWIFT'S ADAPTIVE DLP TO THE MIDDLE EAST

Regional cybersecurity-focused

valued-added distributor, CyberKnight has announced a new partnership with Clearswift, a HelpSystems Company, to further help regional organisations secure critical information.

According to a Gartner, 90 percent of organisations will implement at least one form of integrated data loss prevention (DLP) by 2021, an increase from 50 percent from current figures. In addition, recent Gartner research also highlighted that organisations continue to struggle with DLP deployments and complexities.

As part of the new partnership, CyberKnight will deliver Clearswift's Adaptive Data Loss Prevention Platform (A-DLP), which is designed to automatically apply optimal security treatment based on data content, context and required regulation policy. This includes real-time redaction, encryption,



blocking or deleting. Adaptive DLP offers a unique ability to only remove sensitive information and malicious content passing in and out of the network without the need for human intervention, delays, and quarantines while eliminating false positives.

"Through the partnership with Clearswift we make critical information protection practical for regional customers that are faced with limited IT resources, and encounter more complex cyber threats and compliance regulations," said Avinash Advani, founder and CEO, CyberKnight Technologies.

BEYONDTRUST SECURES MAC AND WINDOWS ENDPOINTS WITH SAAS OFFERING

DAN DEROSA, BEYONDTRUST



BeyondTrust has announced that its BeyondTrust Privilege Management for Windows and Mac solution is now available as SaaS (software-as-aservice), enabling organisations to stop malicious attacks by enforcing least privilege on endpoints, while benefiting from the low total cost of ownership, rapid time to value, and reduced administration burden of a SaaS solution.

As organisations are challenged to secure endpoints that are now in employees' homes, BeyondTrust Privilege Management for Windows and Mac allows them to secure user devices and limit privileges without hindering productivity or driving up calls to the service desk. The SaaS version can be deployed very quickly, and the unique QuickStart capability enables overnight policy implementation across all users, or groups of users, to immediately reduce the risk of unmanaged endpoints.

"With full management capabilities in the cloud, BeyondTrust provides nearly 3,000 customers the best the cloud has to offer – high availability, security, access, and scalability," said Dan DeRosa, Chief Product Officer at BeyondTrust. "As organisations adjust to manage the increase in remote endpoints on the network, BeyondTrust's SaaS solutions feature rapid deployment while also allowing the flexibility only a subscription model can provide."

SOPHOS ENHANCES EDR OFFERING



SCHIAPPA SUDHUZ

ΠΔΝ

Sophos has unveiled an updated

version of its Endpoint Detection and Response (EDR), the first solution designed for both security analysts and IT administrators, available now in Sophos Intercept X Advanced and Intercept X Advanced for Server with EDR. Significant advancements and new capabilities make it faster and easier than ever before for security analysts to identify and neutralize evasive threats, and for IT administrators to proactively maintain secure IT operations to reduce risk.

"Cybercriminals are raising the stakes, stopping at nothing to capitalise on expanded attack surfaces as organisations increasingly move to the cloud and enable remote workforces. Servers and other endpoints are all too insufficiently protected, creating vulnerable entry points that are ripe for attackers to exploit," said Dan Schiappa, chief product officer, Sophos. "Sophos EDR helps identify these attacks, preventing breaches and shining light on otherwise dark areas. Live querying capabilities only available with Sophos EDR in Intercept X enable organizations to search for past indicators of compromise and determine the current system state. This level of intelligence is critical in understanding changing attacker behaviors and reducing attacker dwell time."

Dimension Data has announced that

it will be offering Incident Response Remediation assistance at no cost to UAE hospitals combatting the pandemic.

Expertly designed to effectively contain and mitigate threats, Dimension Data's service will enable affected UAE hospitals to rapidly restore operations after a successful cyber-attack and thus continue to deliver critical services to patients. Public and private hospitals as well as acute care hospitals, urgent care clinics, community health centres, and other emergency care settings are all eligible to 40-hours of incident response support, at no cost, on the condition that they are directly providing care

REDOUANE GAOUAR. DIMENSION πατα

DIMENSION DATA HELPS UAE HOSPITALS

DEFEND AGAINST COVID-19 CYBER-ATTACKS



to COVID-19 patients.

Redouane Gaouar, Director Go-to-Market Practices and Strategic Partner Alliances. Dimension Data Middle East. said, "By offering our Incident Response service at no cost , our intension is to get front line doctors and nurses as well as all supporting functions trying to work in a compromised hospital, back to saving lives as quickly as possible."

WESTCON ME HOSTS VIRTUAL PARTNER SUMMIT ON F5 NETWORKS SOLUTIONS

Westcon has announced the success of

its 'Virtual EDGE Partner Summit'. which highlighted the latest offerings from F5 Networks for its partners across the Middle Fast

The two and half hour virtual event, which was held on 7th May, was attended by over 148 channel executives from across the region. 'EDGE' stands for Engage, Develop, Grow and Extend and is the framework that Westcon consistently follows while building its valueadded offerings throughout the sales engagement journey with partners.

During the virtual event, executives from Westcon delivered a session enlightening partners about solutions from F5 Networks that address the current market requirements along with session on Westcon's digital distribution capabilities and how it can assist them in the current challenging times. During the summit, the guests were kept engaged and entertained through

STEVE LOCKIE. WESTCON-COMSTOR ME

live guiz competitions, raffle draws and celebrity magic performance.

Westcon also highlighted its Marketing as-a-Service (MaaS) initiative, which can help the partners in generating demand through a wide range of marketing services. The success of the campaign has encouraged Westcon to extend the MaaS offerings to its extended partner base.

Steve Lockie, group managing director, Westcon-Comstor Middle East, said, "The focus of the summit was to help the channel partners become aware of the technology segments which are currently in demand and how we can support them in these challenging times. We remain committed to helping our partners by providing them unhindered support and services."

EXCLUSIVE NETWORKS ME, CHECKMARX INK DISTRIBUTION DEAL

Exclusive Networks ME has announced its partnership with Checkmarx, a software security solutions firm for DevOps.

Under the partnership, Exclusive Networks will deliver Checkmarx's Software Security Platform to customers in the Middle East.

The strategic partnership will allow Exclusive Networks to expand its cybersecurity portfolio and business scope to provide industryleading application security testing (AST) solutions that can empower regional organisations to remediate vulnerabilities throughout the software development lifecycle (SDLC) more NATHAN CLEMENTS, EXCLUSIVE NETWORKS ME



efficiently and effectively.

"Our mission is to stay relevant and drive innovation within our channel ecosystem. Our partnership with Checkmarx allows us to do this. Organisations today are rapidly realising the risks that arise during the software design and coding phases and are turning to application security testing solutions to help them reduce these vulnerabilities," said Nathan Clements, General Manager, Exclusive Networks ME.

Checkmarx offers automated security scanning as part of the DevOps process. The Checkmarx Software Security Platform integrates SAST, IAST, SCA, and developer application security awareness and training solutions, enabling organisations to elevate their software security postures. The solution is available on-premises, in the cloud, or for hybrid environments.

STARLINK PENS DISTRIBUTION DEAL WITH BEYONDTRUST FOR ME AND LEVANT



NIDAL OTHMAN, STARLINK AND JOHN HATHAWAY, BEYONDTRUST

Dubai-based VAD StarLink has

signed a distribution partnership with BeyondTrust for Middle East and Levant.

According to both companies, the alliance will allow them to collaborate and provide customised Privileged Access Management (PAM) solutions that meet the unique requirements of enterprises in the region.

Global PAM solutions provider BeyondTrust offers a seamless approach to preventing data breaches and empowers enterprises to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps and network device environments. The PAM vendor providers a holistic platform and offers flexible design that simplifies integration and enhances productivity and maximises IT and security investments. Nidal Othman, co-founder and managing director, StarLink said, "We are at an age where cyber-attacks are unpredictable, and organisations are at a constant risk from internal and external threats which makes PAM a crucial part of the security infrastructure. Our capabilities in the Privilege and Identity Management domain makes us the 'Distributor of Choice' and we are delighted to take this partnership to a new level."

"Driven by an increasing customer demand for PAM solutions, over the last couple of years, we have expanded our direct footprint across the region. To ensure we can serve customers in all our key markets, it is essential that we work closely with a security focused distributor that can match our regional coverage, has a strong infrastructure, partner network and in-house technical and consultancy resources. StarLink ticks all these boxes and I look forward to building a long-standing, mutually beneficial relationship as we continue to execute on our aggressive growth plans for the region," said John Hathaway, regional vice president, Middle East & India, BeyondTrust.

VERITAS Ransomware

Paying hackers is a losing game.



of consumers believe that hacked companies should stand up to cybercriminals and refuse to pay ransoms.



of consumers demand compensation from the company if they can't restore their data.



per affected person is the average ransom consumers believe companies should pay to retrieve their data.

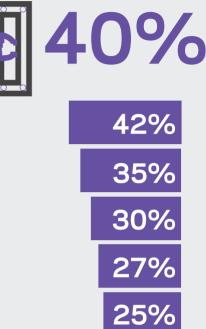


of consumers would stop using the company's services no matter what it decided.

Methodology: Interviews conducted and statistics compiled for Veritas Technologies LLC by 3Gem. A total of 2,000 consumers were interviewed in April 2020 in each market (China, France, Germany, Japan, United Kingdom and United States) adding up to a global sample size of 12,000 adults over the age of 18.

Copyright © 2020 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and Backup Exec are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. V1053 6/20

Demanding sanctions against CEOs.



of consumers blame CEOs personally if their companies are breached by ransomware.

ask for a public apology.

want the CEO to pay a fine.

demand the CEO be banned from running a company in the future.

demand the CEO resign.

want the CEO to take a pay cut or be demoted.

demand a prison sentence.

Back up, don't pay up.

23%



of consumers expect companies to implement security software to protect their data.



62%

of consumers expect companies to have tried-and-tested backup copies of their data.

These steps allow companies to ward off ransomware attacks or at least restore data after an attack without paying a ransom.

WHY PASSWORD HYGIENE MATTERS

IF THERE'S A VALID REASON TO CHANGE ONE OF YOUR PASSWORDS, DO IT RIGHT AWAY TO STAY AHEAD OF THE CROOKS, SAYS **PAUL DUCKLIN**, PRINCIPAL RESEARCH SCIENTIST, SOPHOS.

ntil a few years ago, everyone received advice to change passwords on a regular and frequent basis, just because it was possible. But the idea was to reduce the length of time you'd be exposed if your password were breached since passwords provide the first line of defense to your personal and business devices.

Are password resets needed at all?

By all means, change your passwords whenever you like if you want to – and if you use a password manager, it's easy to do just that.

But the only time you should feel compelled to change a password is when there is a clear and obvious reason to do so, and that's if you think – or, worse still, know – that it might have been compromised.

Fortunately, in many or most recent data breaches (not all) where authentication data gets stolen, the crooks don't end up with your actual password along with your login name.

Passwords usually are – or certainly should be – stored in a hashed form, where the hash can be used to verify that a supplied password is correct, but can't be wrangled backwards to reveal what the password was. As a result, most password exposures that arise from data breaches require that the crooks first crack your password by trying a long list of guesses until they find one that matches your password hash.

Simply put, the longer and more complex your password, the longer it will take for the

crooks to crack it. They try the most obvious passwords first, so **123456** will probably be the very first one they try for each user; **Pa55word!** might be the 100,000th on their list; but they are unlikely to get around to trying **VFRHFMNOLR5LAIVGDOW5UZRT** for days, or months, or even years.

In other words, if a service provider notifies you that your password hash was acquired by crooks, you'll nevertheless remain safe if you change your password before the crooks get around to cracking it.

Even if the breach happened weeks or months ago, you've probably still in a good position to beat the crooks to it, assuming you choose wisely in the first place – and if you use a password manager, it's easy to do just that.

How quick are we?

A paper entitled (How) Do People Change Their Passwords After a Breach? that came out recently from Carnegie Mellon University in the US reveals that that a worrying number of us aren't quick at all. The researchers found that very few of their participants reported intentions to change passwords after being notified that their passwords were compromised or reused, including because they believed in the "invincibility" of their passwords.

How good are we?

Disappointingly, even for the one-third who did change the relevant password, most took more than three months to get around



to it, and many of those replaced their old passwords with weaker ones.

Even more intriguingly – though perhaps, with hindsight, not surprisingly – the researchers claim that those who did change passwords tended, on average, to pick a replacement that was more similar than before (measured by substring similarities) to all their other passwords.

In short, humans really aren't good at randomness – but then, they aren't very good at reacting to data breach advice either.

What to do?

- Don't delay, do it today
 If there's a valid reason to change one of
 your passwords, do it right away. This will
 keep you ahead of the crooks
- Avoid taking shortcuts
 Choose quality passwords. Crooks will spot
 any tricks or patterns you use in order to make
 your passwords different yet similar enough to
 remember easily. If you have u64b2vqtn5-fb
 for Facebook and u64b2vqtn5-tw for Twitter,
 the crooks will figure out the rest of your
 passwords with ease.
- You are not invincible
 The crooks probably won't
 crack your password if it's
 6GHENBIZMX3TTUHJTPQZTEKM, but why
 take the risk that they might?
- 2FA as an excuse won't help Don't use 2FA as an excuse to choose a trivial password or to use the same one everywhere

 it's meant to be a second factor, not just a different sort of single factor.

NAVIGATING CYBERSECURITY IN THE 'NEW NORMAL'

84% OF BUSINESSES ARE SET TO INCREASE WFH CAPACITIES BEYOND THE PANDEMIC DESPITE SECURITY WOES

espite security issues and concerns resulting from the massive and sudden increase in work-from-home (WFH) initiatives caused by the global COVID-19 healthcare crisis, one-third (38%) of U.S. companies observed productivity gains during remote work and a staggering 84% anticipate broader and more permanent WFH adoption beyond the pandemic, according to new data today released by Pulse Secure, the leading provider of software-defined Secure Access solutions.

Cybersecurity

The 2020 Remote Work-From-Home Cybersecurity Report, sponsored by Pulse Secure and produced by Cybersecurity Insiders, offers an in-depth perspective on WFH challenges, concerns, strategies and anticipated outcomes. The survey, conducted in May of 2020, polled over 400 IT security decision practitioners across a broad representation of industries and companies between 500 and over 5,000 employees. The survey found that 33% of U.S. companies anticipate some positions moving to permanent remote work and over half (55%) plan to increase their budget for secure remote work in the near-term.

WFH adoption accelerated cloud app growth and business continuity challenges

The research indicates that three-quarters of businesses now have more than 76% of their employees working from home compared to just under 25% at the close of 2019. While a third of respondents cited their business being "ill prepared or not prepared" for remote working, 75% of businesses were able to transition to remote working within 15 days. Surprisingly, less than a third expressed cost or budget problems, demonstrating the urgency to support their business. Additionally, more than half (54%) expressed that COVID-19 has accelerated migration of users' workflows and applications to the cloud.

Increase in WFH employees fuels security and compliance issues

In terms of security risks, two-thirds (69%) are concerned

with WFH security risks with the majority expressing low user awareness training, insecure home/public WiFi networks, use of at-risk personal devices and sensitive data leakage as prime threat contributors. In terms of application exposure, respondents feel anxious over file sharing (68%), web apps (47%), and video conferencing (45%) risks.

While 78% expressed enforcing the same level of security controls and data management for on-premise and remote users, a further 65% allowed access from personal, unmanaged devices. Two-thirds of IT security professionals anticipate malware, phishing, unauthorised user and device access, and unpatched/at risk systems to be the most exploitable WFH attack vectors. In addition, 63% expressed that remote work could impact compliance mandates that apply to their organisation; especially GDRP, PCI-DSS, HIPAA and those with data breach notification.

Wider trends toward security tools consolidation

Survey respondents employed various tools to secure remote work / home office scenarios with the top four controls being endpoint security, Firewalls, virtual private networks (SSL-VPN) and multi-factor authentication (MFA). According to separate research by Enterprise Management Associates, 57% of organisations regard the consolidation of access management solutions into a single platform to be a high or extreme priority for their business this year.

The WFH and tool consolidation trends coincide with a recent update to Pulse Access Suite, a secure access solution set that provides easy access for mobile workforces and a single-pane-of-glass to streamline provisioning, management and scalability. The Suite integrates adaptive identity and device authentication, protected connectivity, extensive visibility and analytics, and threat response for hybrid IT. Organisations can centrally orchestrate Zero Trust policy to ensure compliant access to applications, resources and services across mobile, network and multi-cloud environments.

OF ORGANISATIONS EXPRESSED CONCERNS AROUND WFH SECURITY RISKS

To learn more about the Pulse Secure and explore additional 2020 Remote Work-From-Home Cybersecurity Report findings, please visit: http://www.pulsesecure.net/WFH_cybersecurityreport/

SMART VISION

WITH ITS DECADE-STRONG EXPERTISE AND CAPABILITIES, HYVISION TECHNOLOGY IS AMONG THE KEY PLAYERS DELIVERING ROBUST AND INNOVATIVE SMART VIDEO SURVEILLANCE OFFERINGS TO REGIONAL BUSINESSES. IN AN EXCLUSIVE INTERVIEW, THE FIRM'S GENERAL MANAGER **LEO LIAO** SHARES INSIGHTS INTO THE EVER-EVOLVING SMART VIDEO SURVEILLANCE MARKET AND WHY CUTTING-EDGE STORAGE IS PERTINENT FOR SUCCESSFUL IMPLEMENTATIONS. s nations across the region continue to invest heavily in smart and safe city technologies, they are increasingly putting their attention

and investments into video surveillance solutions. According to Marketsandmarkets, the global video surveillance market is expected to reach \$74.6 billion in five years, signifying that it will continue to grow as organisations recognise the importance of investing in this security segment. In line with this, industry insights have also predicted that the global video surveillance storage industry is poised to reach \$58.31 billion by 2027, as securely storing critical data obtained from surveillance cameras becomes vital.

Hyvision Technology is the national distributor of Hikvision solutions in the Gulf. As a security-focused valueadded distributor, the organisation has grown from strength-to-strength, owing to its holistic spectrum of optimal surveillance solutions and

"OUR STRONG CAPABILITIES AND VAST KNOWLEDGE ON SMART VIDEO SURVEILLANCE TECHNOLOGIES ARE WHAT SETS US APART IN THE INDUSTRY."

expertise in catering to a wide range of industries from government to banking, education and hospitality.

Leo Liao, general manager, Hyvision Technology (HTL), discusses how smart video surveillance technologies have evolved to deliver benefits beyond security, and highlights how their partnership with Seagate has enabled them to deliver reliable and innovative offerings.

Please give an overview of Hyvision's operations.

Hyvision Technology, which is also known as HTL, has been in the security surveillance industry for more than a decade. Headquartered in Dubai, Hyvision is the strategic national distributor for Hikvision catering to UAE, Oman and Bahrain markets. We have extensive industry expertise and have established a robust channel network. Our strong capabilities and vast knowledge on smart video surveillance technologies are what sets us apart in the industry. These qualities have leading value-added distributors of perimeter security products and

Can you elaborate on your partnership with Seagate?

Seagate Technology is a global leader in data storage and management solutions. With more than 40 years of research and innovation under its wing, Seagate is among the pioneers in data storage. They have a vast understanding of the requirements surrounding the smart video surveillance as well as the data management challenges that this market can face.

Through our partnership with Seagate, we were able to achieve synergy, which has been mutually importantly, this strategic partnership has also brought significant advantages to our partners, by making Seagate solutions more accessible. As part of the partnership, we are products, including the Seagate SkyHawk product line, which is designed specifically for video surveillance needs. We are also utilising Seagate's Enterprise-level storage capacity and performance efficiencies while ensuring robust data security.

What were the specific factors that led you to choose Seagate as your storage partner?

We believe Seagate is synonymous with security, reliability, and data protection. They have top-notch expertise and capabilities in improving security and innovations for surveillance-optimised solutions.

Moreover, they offer a wide array of power-saving and cost-effective products that have been designed to not only keep data safe but also provide prompt access to analysis. On the technical side, we've seen that their products provide the highest throughput required to support high-performance continuous data processing, advanced caching mechanisms, instant response and superior random read speeds.

But beyond that, we saw first-hand how dedicated they are to quality assurance. They conduct over 160 rigorous quality tests. They also measure various aspects of quality from the time a hard drive from the product conceptualisation stage to the design, and through a product's 'end of life.' They also ensure that they support their partners like us by ensuring stock availability and other provisions such as a credit facility, delivery to door service and RMA services.

Can you please share some of the most notable projects that you have implemented together with Seagate?

Most recently, Hyvision, together with Hikvision and Seagate, have embarked on a project for GEMS Education. GEMS is an international education company. It is a global advisory and educational

Zubair Shareef, Surveillance Solutions Sales Manager, Seagate

UAE, explains why storage is instrumental in the success of smart video technologies and how the organisation is supporting partners such as Hyvision.

How has the smart video surveillance industry evolved over the years?

The paradigm within the security and surveillance industry has shifted from VCR based analogue CCTV (Closed-circuit television) to network-based systems. This has given rise to a trend wherein we see consumers moving away from physical security and adapting to video-based security AI-enabled surveillance camera technology. Moreover, AI-enabled networkbased cameras are being used to ensure high levels of production quality and efficiency, safety management, traffic management and more.

How important is the role of storage technologies in the growth of this market segment?

Video is no longer a security-only proposition. Many industries rely on video, analytics and AI to provide insight that guides business decisions or otherwise streamlines various operations. With all this in mind, video storage can no longer be an afterthought – it is a vital part of the planning, design and deployment of surveillance



systems. One of the main criteria integrators should use for selecting storage solutions is hard drive capacity, but reliability and durability are also important considerations.

Considering the potential consequences of lost video frames or drive failure, the lowest-priced storage solutions can ultimately turn out to be expensive in terms of liability, legal and other ramifications. Thus, it makes sense for integrators to choose surveillance-optimised storage solutions built for 24x7 operation, which also has AI design and build drives that offer health-monitoring capabilities (SHM).

What kind of support does Seagate provide to partners such as Hyvision?

Our strategic partners like Hyvision, are an extension of our business. We support them by engaging and providing the right tools in terms of training, marketing and go to market plans. This support brings the Seagate technology and offerings closer to the market and world of security solutions.



management firm and is the largest operator of kindergarten-to-grade-12 schools in the world.

The project entailed installing Hikvision cameras and a variety of VMS solutions across 45 GEMS Schools

in the UAE. We installed between 200 to 500 cameras per school and deployed a variety of VMS solutions such as HIK Central, Hikvision NVR, Dell Server and IBM Storewise. All these VMS servers have been equipped with different capacities of SkyHawk HDDs from Seagate and have been configured on different types of RAIDs.

The project has brought the customer significant benefits such as increased security and operational efficiencies.

4.6

VALUE OF GLOBAL SMART VIDEO

SURVEILLANCE MARKET BY 2025

SOURCE: MARKETSANDMARKETS

In addition, with the Seagate HDD-equipped VMS's they did not face any issues in data retrievals, performance and backup and archiving.

> The COVID-19 pandemic has significantly impacted organisations across the region.

As businesses transition to a new way of living, how can smart video technologies deliver benefits beyond security?

As the pandemic affects business operations and the way of living today, we believe smart video technologies can play a vital role in enhancing the precautionary measures in stemming the outbreak. In line with this Hyvision, is well-positioned to provide a variety of cameras and smart video solutions with thermographic technologies to measure temperature, detect the use of masks and keeping social distance.

As an example, for shopping malls, we provide thermal cameras to detect body temperatures and facial masks at the entrance. We also offer facial recognition access control

COVER FEATURE



terminal for staff offices to measure temperature and detect masks with basic staff attendance as well as access authentication tools. In addition, we provide handheld thermal cameras for security staff who are patrolling parking areas when people are sitting in a car.

In terms of ensuring social distancing within establishments, we offer solutions for controlling the flow of customers with digital signage solutions, which have also been integrated with temperature screening, mask detection and density control function.

As a smart video surveillance player, this is how Hyvision is responding to the impact of the pandemic. We are committed to helping people stay safe and leveraging our solutions to help businesses to get back on track while staying secure and safe.

How do you think will the video surveillance space evolve? And along with that, how will storage requirements evolve as well?

We witnessing a significant rise in artificial intelligence (AI) and Internet of Things technologies today. These technological trends are increasingly being integrated into a multitude of smart video products and solutions. For example, we offer AI cameras, that enable facial detection and recognition, vehicle and non-motor vehicle detection, vehicle brand recognition, pedestrian detection, human body feature detection, abnormal facial detection, crowd behaviour analysis, multiple target tracking and more.

We believe that video surveillance will evolve into a smart facility for visualised insightful management and data analysis, that will bring vast benefits beyond just surveillance security. With this evolution, there will be an increase in demands for data storage products that can provide faster process speed, higher clarity and safer data protection as well as other innovations that can keep up with the transformation of the market as a whole.

"WE BELIEVE SEAGATE IS SYNONYMOUS WITH SECURITY, RELIABILITY, AND DATA PROTECTION."

Barracuda Cloud Security Guardian

Build fast. Stay secure.

Remove security as a burden in the cloud.

Developers like the speed and flexibility of the cloud—but many fail due to cloud security challenges. Cloud Security Guardian manages security for them, automatically.

Leverage industry best practices for security compliance.

Cloud Security Guardian is fully CIS Benchmarks-certified – their benchmarks are incorporated as pre-loaded policies in Cloud Security Guardian. Policies for PCI DSS and HIPAA are also included.

Full-stack cloud security.

Only Barracuda Networks integrates cloud security management with perimeter and network security solutions – i.e., control, data, and management plane security together in a single solution.

For more information visit: barracuda.com/products/cloudsecurityguardian or contact: MET_sales@barracuda.com

80 percent of cloud breaches are self-inflicted.

"Through 2020, 80 percent of cloud breaches will be due to customer misconfiguration, mismanaged credential, or insider theft."

Gartner Research



A SAFE SPACE

SUMEDH GANPATE, SENIOR COLLABORATION PRACTICE LEADER, AVAYA INTERNATIONAL, GIVES *SECURITY ADVISOR ME* A LOWDOWN ON HOW THE COMPANY IS INNOVATING TO MAKE AVAYA SPACES NOT ONLY A RELIABLE BUT ALSO A SECURE PLATFORM FOR TODAY'S REMOTE WORKFORCE.

remote working schemes, virtual meeting apps have gained significantly.

Avaya was among the first companies to open its innovative collaboration software – Avaya Spaces – offering a 60-days free licence, to help businesses, as well as education institutions worldwide, adapt to remote working.

At a time when organisations are easing into the 'new normal' and the use of video collaboration solutions is becoming

"SECURITY, PRIVACY AND INTEGRITY ARE CRITICAL TO AVAYA AND OUR RELATIONSHIPS WITH OUR CUSTOMERS."

mainstream, many are voicing their concerns about the security of such applications. Sumedh Ganpate, Senior Collaboration Practice Leader, Avaya International, any enabling

ormal life as we know it has come to a sudden halt during the first quarter of the year due to the COVID-19 pandemic.

The precautionary measures against the spread the outbreak has pushed businesses across multiple sectors to re-think the way they operate to ensure business continuity.

The rise of video conferencing apps has been one of the defining elements of the coronavirus pandemic. With companies across the globe forced to implement discusses how the company enabling secure and scalable enterprise collaboration with Avaya Spaces.

As organisations continue to adapt to new working environments, they become increasingly reliant on cloud solutions, what key best practices can they adopt to avoid any security gaffes in choosing the right platform?

Cloud-based solutions enable rapid, hassle-free deployment, and in recent months have proven to be an attractive option for businesses looking to rapidly roll out work-from-home strategies without having to incur prohibitive upfront overheads.

While this has largely been beneficial for businesses, as rapid uptake of tools may provide a quick solution to organisations looking to expediently roll-out remote working initiatives, they could impede an organisation's longterm success. By rapidly rolling out new tools, businesses are encouraging their employees to adapt to new technologies and consequently become dependent on new ways of working. For example, given employees' familiarity with consumergrade video collaboration solutions, it may be easy to now get them to use these when communicating and collaborating with their colleagues and customers. However, these solutions often lack the security, scalability and features that are essential to true enterprise collaboration. Once procedures have been set and behaviours adopted, changing them could be a major challenge. We've learned this lesson before with the rise of shadow IT and even today, IT teams battle to ensure employees use official file sharing applications rather than unregulated alternatives such as personal email, USB drives or cloud-storage applications.

When choosing the right enterprisegrade collaboration platform – whether cloud-based or otherwise - organisations need to evaluate key security criteria. As basic requirements, the platform should implement industry-standard end-to-end encryption. For example, Avaya Spaces is built on a secure and trusted solution, with Google Cloud data encryption at rest. There's also in-transit SAML and OAuth 2.0 support for secure login and GDPR compliance retention policies built-in. As has been clear from media reports in recent months, unauthorised entry can be a prime concern which is why user authentication and password protected entry to meetings are also essential security features.

In terms of the level of security, what differentiates Avaya Spaces as a platform as compared to its counterparts in the market?

Our customers rely on Spaces to maintain business continuity and some of their most important strategy meetings are held on this application, with sensitive data being shared via the solution's convenient file sharing functionality. They have the confidence to do this because they know that security is a top priority at Avaya - we have designed Spaces from the ground up with security in mind at every step. Spaces is built on the Google Cloud and data is stored on the Cloud back-end application. Data required by Spaces is stored in encrypted form via Google Cloud. Data required by the browser client is stored in the browser itself in the form of cookies or in the cache. Data required by the mobile application is stored on the mobile application container service provided by the OS and recent mobile OS versions support encrypting application container data. Moreover, when data is being transmitted by Avaya Spaces over a network, it is encrypted.

What does it mean to receive a BCR approval for Avaya Spaces?

Avaya was one of the first companies in its sector to achieve the Binding Corporate Rules (BCR) approval from European Union data protection authorities. Successfully completing BCR compliance is a testament to the standards Avaya has set in handling personal data and in upholding fundamental privacy principles, such as data security, quality and transparency.

Protecting the personal data of our stakeholders will always be a top priority for Avaya and the endorsement by the EU data protection authorities demonstrates that we are committed to achieving the highest standards.

How have you ensured to keep the balance between data privacy, ease-of-use and productivity for the users?



Security, privacy and integrity are critical to Avaya and our relationships with our customers. Like all other Avaya solutions, Avaya Spaces is compliant to data-privacy regulations including the EU GDPR law. This reinforces customer's confidence that their personal data is protected. Meeting data is secured and encrypted by Spaces and stored on Google Cloud Platforms, which are natively encrypted by nature, ensuring a double layer of protection. However, the backend security and privacy don't sacrifice the intuitiveness of Avaya Spaces, which delivers a simple, easy-to-use experience. All these factors make Avaya Spaces a simplified productivity tool for secured team collaboration.

Can you please give an overview of the latest enhancements to Avaya Spaces' security features? What was the driver behind the addition of the new 'Private Space' setting?

A "Private Space" uniquely prevents any intruder or unintentional participants trying to join the meeting as a "Guest". Only authorised "Members" and "Admin" users invited by the group owner are allowed to join private meetings and can collaborate securely. This eliminates any intentional or unintentional access to Spaces meetings. On top of Private Spaces, any Spaces user who wants to secure their meetings further can password-protect their Spaces.

Why is it important to regularly update the security features of platforms such as Avaya Spaces? What other security features are you looking to roll out in the future? The demand for group collaboration apps such as Avaya Spaces has spiked in the past few months due to COVID-19 pandemic. For the majority of Avaya Spaces users, this tool is used for pivotal activities, discussions and decision making. Therefore, it's natural to expect highest possible security standards. And we continue to enhance these standards as the nature of Spaces usage intensifies.

We have plans to extend security features to our video endpoints, including the Avaya Collaboration Unit CU360 & XT devices. More importantly, Spaces APIs and SDKs are being buffed up to allow Spaces to integrate with customer's existing portals or applications, leveraging any existing security features embedded within.

HOW SMART VIDEO TECHNOLOGIES HELP MAINTAIN SOCIAL DISTANCING

HEALTH ORGANISATIONS AROUND THE WORLD HAVE CREATED THE COMMON AWARENESS THAT MAINTAINING A SAFE DISTANCE BETWEEN PEOPLE IS ONE OF THE BEST PRACTICES WE HAVE TO AVOID BEING EXPOSED TO COVID-19 AND IN SLOWING ITS SPREAD. **HIKVISION** SHARES INSIGHTS INTO HOW SMART VIDEO TECHNOLOGY CAN HELP CURB THE OUTBREAK.

s various countries and regions push to reopen businesses and relax stayat-home orders, social distancing remains an ongoing requirement. More than that, crowd density information is also considered a significant reference in managing the "social distance" of workplaces, businesses and public spaces.

Business owners are working hard to keep employees, customers and visitors protected. Dealing effectively with 'density' – a new imperative for management and operations – complicates staffing and interpersonal interaction.

Limiting the number of people to ensure safety

In the current situation, public and private managers and authorities have to do more than ever before to keep people safe, and in many cases efficient calculation of customer traffic will be essential.

Hikvision's Flow Control Solution uses people counting cameras and digital signage, which provides a dynamic on-screen display to show users how many people are entering and leaving a building or an area, and sends real-time alerts in case pre-defined capacity thresholds are exceeded. These people counting camera utilise highly accurate 3D binocular stereo vision and Deep Learning algorithms, making complex counts easy, even in multi-door sites.

More important, the Flow Control Solution can be easily and rapidly deployed. It is designed to be simple to use and highly accurate, with options to suit all potential application scenarios. In locations with a single entrance, one people counting camera can be installed at the entrance and connected to digital signage. For multi-entry scenarios, people counting cameras can be installed at each entrance and exit, equipped with I-Series NVRs or HikCentral to calculate numbers of people entering or leaving, so as to accurately provide real-time number data.



"AS BUSINESSES BEGIN TO EMERGE FROM LOCKDOWN, THEY NEED TO FIND WAYS TO REDUCE RISKS OF FURTHERING THE SPREAD OF THE VIRUS."

For example, a supermarket can install a clear and easy-to-understand, dynamic data number display at each entrance to provide real-time updates for people waiting to enter. An alert is generated when the pre-configured maximum is reached, and an audio alarm can be triggered if anyone attempts to enter before the numbers go below that threshold.

At present, with expenses more critical than ever, users can use the Flow Control Solution to automatically monitor the situation, empowering businesses and possible reducing the required number of security guards and other resources.

Maintaining a safe social distance in public

In areas where crowds are unavoidable, such as cash registers in supermarkets and the ticket kiosks at public transportation hubs, managing distances



Multiple entries and exits

between people queuing (standing in line) is also critical. Authorities in various locations have established specific guidelines and legislation in this area, balancing needs and risks for citizens.

Hikvision Dual Lens Cameras (DS-2CD6825G0/C-I(V)(S)) help retail stores and other businesses measure social distancing, and its advanced 3D binocular stereo vision and deep learning algorithm can be configured to trigger alarms according to local regulations and requirements. Users can set the minimum contact distance threshold needed; when the distance becomes less than this preset threshold, an instant alarm and popup will appear with audio and video linkage.

And there's more...

Alongside the Density Control Solution, Hikvision also offers a Mask Detection Solution. This technology ensures that anyone entering a premise is wearing a face mask when they are required to do so. Those without a mask will not be granted entry.

The Mask Detection Solution can be delivered in a variety of formats depending on user needs: added to a specialty camera or a Hikvision DeepinMind NVR for users with existing camera systems, integrated into Hikvision's Temperature Screening Thermal Solution, or as part of a MinMoe door access unit with built-in face detection technology. Entry can be denied if a mask is not worn and/or an out-of-range skin-surface temperature is detected.

As businesses begin to emerge from lockdown, they need to find ways to reduce risks of furthering the spread of the virus. This affects whole populations and all their normal activities – from getting coffee on the way to work and boarding public transportation, to shopping and eating out. But there are some technologies that they can turn to – innovations that will facilitate a 'new normal' and keep people safe. And Hikvision will be there, every step of the way.

FINDING THE UNKNOWN

ANAS JWAIED, MANAGING DIRECTOR, MIDDLE EAST & AFRICA AND **TAMER EL REFAEY**, CHIEF CYBERSECURITY STRATEGIST, EMERGING MARKETS, MICRO FOCUS, DISCUSS HOW ARCSIGHT INTERSET UEBA ACCELERATES THREAT DETECTION AND BOLSTER SECURITY STRATEGIES.

ybersecurity threats can come in many forms and are ever-evolving. Oftentimes, businesses tend to focus on preventing and mitigating external threats, that they overlook the vulnerabilities that are closer to home - insider threats. However, contrary to popular belief, not all insider threats are those rogue employees who seek financial gain, sometimes it is the unsuspecting and non-malicious ones that put your systems at risk. Employees, contractors, partners, and privileged users can all become insider threats. And since not all of them may put the organisations at risk maliciously, they are tough to spot.

User and entity behaviour analytics (UEBA) empowers security teams to identify and detect those tough-to-spot threats. It provides organisations with a comprehensive way to implement top-notch IT security, while also helping detect users and entities that might lead to entire system compromise.

"Businesses today have countless

Anas Jwaied Managing Director, Micro Focus "ARCSIGHT INTERSET IS UNIQUELY POSITIONED TO FIND THE THREATS THAT MATTER FOR ENTERPRISES WITH VALUABLE DATA TO PROTECT, LIMITED SECURITY OR FINANCIAL RESOURCES AND SIGNIFICANT ATTACK SURFACE TO MONITOR." critical assets to protect such as customer information, intellectual property and critical infrastructure among others," says Anas Jwaied, managing director, Middle East and Africa, Micro Focus. "Unfortunately, traditional approaches are no longer sufficient in protecting assets. This leaves security teams struggling with fragmented security ecosystems, unreliable analytics and a never-ending barrage of false alarms. Meanwhile, business leaders expect security teams to flawlessly protect against critical threats while also delivering new innovations to enhance the organisation's security posture."

ArcSight Interset UEBA gives security leaders a new lens through which they can detect, hunt, investigate, and respond to threats that may be hiding in the enterprise—before data is stolen.

"ArcSight Interset is uniquely positioned to find the threats that matter for enterprises with valuable data to protect, limited security or financial resources and significant attack surface to monitor," says Jwaied. "By effectively identifying and prioritising cyber threats, ArcSight Interset allows security teams to use their resources more strategically."

Using unsupervised machine learning, ArcSight Interset UEBA filters huge volumes of threat data and events. It prioritises them into a list of highquality security leads to streamline and accelerate the efforts of your security operations centre (SOC). ArcSight Interset's unsupervised machine learning models, is equipped with an intuitive user interface (UI), which allows security leaders to simplify and fast-track threat detection and investigation.

"ArcSight Interset UEBA bypasses conventional rules and thresholds and instead assesses the potential risk of a user or entity in your enterprise using scientific mathematical algorithms and autonomous machine learning models,"



says Tamer El Refaey, chief cybersecurity strategist, Emerging Markets, Micro Focus. "This approach, combined with ArcSight Interset's native Big Data architecture, allows your security team to detect threats with speed and at scale."

Through unsupervised machine learning, ArcSight Interset's algorithms extract available entities including users, machines, IP addresses, servers, printers and more from log files. It then observes events and evaluates these entities' movements to determine expected behaviour—a measurement called 'unique normal.'

"The UEBA then creates a baseline of these behaviours as new information comes through the analytics process," explains El Refaey. "Once anomalous or high-risk activities are spotted, the events are evaluated against previously observed behaviour to assess deviations and potential risks."

"Using an intuitive dashboard, security teams can measure a user's recorded risk scores over time and view an incident's context in a clear, actionable, interactive interface, thereby, minimising false-positive alerts. This is how ArcSight Interset detects insider threats while enabling security teams to work more quickly and efficiently to mitigate them."

ArcSight Interset's output risk assessments can be leveraged to implement actions via automation, orchestration, and alerting solutions to provide faster responses once risks are found.

ArcSight Interset and MITRE ATT&CK

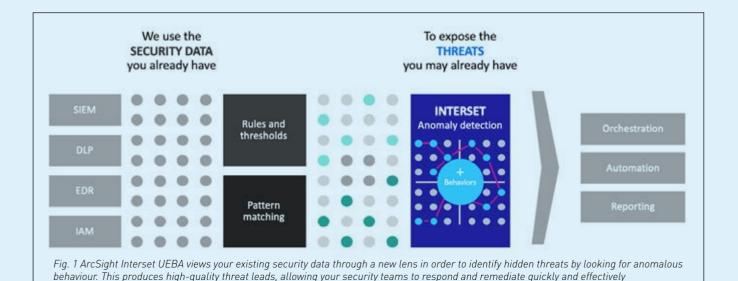
MITRE's ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a comprehensive matrix of threat tactics and techniques observed in realworld attacks on enterprise networks. The framework is leveraged by threat hunters, red teamers, and defenders to better classify attacks and assess an organisation's risk. MITRE ATT&CK plays a pivotal role in ArcSight Interset's UEBA in providing detailed information for effectively protecting organisations against real unknown attacks.

"Today, ArcSight Interset's UEBA covers 75 percent of the tactics and techniques in the ATT&CK framework," says Jwaied. "Our machine learning models are carefully mapped to ATT&CK's 219 techniques. It helps us gain a better view of which attack Tamer El Refaey Chief Cybersecurity Strategist, Emerging Markets, Micro Focus

techniques are our customers most vulnerable to, where ArcSight Interset can effectively provide coverage and how we can leverage our anomaly models to protect businesses against real threats."

Together, ATT&CK and UEBA can identify the links between unusual activity inside your enterprise and real, actionable security threats.

"ArcSight Interset provides security teams with a holistic view of the risks and vulnerabilities they face. For enterprises with valuable data to protect and critical systems to monitor, ArcSight Interset is well-positioned to find the threats that matter — before it's too late," says Jwaied.



www.tahawultech.com

NAVIGATING CHANGE

ANAND CHOUDHA,

FOUNDER AND MANAGING DIRECTOR OF THE SPECIALISED SECURITY DISTRIBUTOR, SPECTRAMI, SHARES INSIGHTS INTO THE CYBERSECURITY CHALLENGES BROUGHT BY THE COVID-19 PANDEMIC AND HOW THE DISTRIBUTOR IS PLAYING A ROLE IN HELPING REGIONAL BUSINESSES NAVIGATE THEM. hat are the biggest security challenges organisations are facing today? With cybercriminals exploiting the COVID-19 pandemic by launching an unprecedented barrage of Covid-19 themed attacks, there has been a big increase in the cyber threats in the past few months. UAE and Saudi Arabia have been among the most-affected countries in the region, accounting for bulk of the Covid-19themed attacks in the GCC.

Over the past few months, we have witnessed cybercriminals taking advantage of people's fears over the coronavirus pandemic. Furthermore, as more people are spending more time online than ever, the has been a significant surge in phishing attacks.

Furthermore, as the current situation impact economies across the globe, many industry verticals have witnessed mass layoffs can be extremely vulnerable to such attacks. At this time and age, nobody is safe from cyber-attacks, be it large, medium, or small enterprises. Even the best of the technology companies has fallen victims to such attacks. Recently, one of the biggest IT services companies in the world, Cognizant suffered a big hit from a Maze ransomware attack.

How has the ongoing COVID-19 pandemic, impacted security strategies and investments?

We have observed that the overall

"AT THIS TIME AND AGE, NOBODY IS SAFE FROM CYBER-ATTACKS, BE IT LARGE, MEDIUM, OR SMALL ENTERPRISES." IT budgets have been cut by approximately 45 percent. However, information security budgets have remained intact. Customers' security strategies have moved from being a 'good-to-have' investment to a 'must-have'. There is an increase demand for technologies that include threat intelligence, endpoint security and those that help in securing remote operations.

Can you please give an overview of Spectrami's cybersecurity offerings?

Spectrami is a Dubai-headquartered pan-EMEA value-added distributor with a local presence in the Middle East, North Africa and parts of Europe. We are a cybersecurity specialist and we work with some of the world's leading cybersecurity vendors offering end-to-end solutions. We're also assisting regional enterprises to meet regulatory standards on their infrastructure, protect confidential data assets and applications.

As a distributor, how do you enable organisations in the region become cyber resilient? What role can Spectrami play in the future of the regional cybersecurity landscape?

It has always been our quest to offer the best-in-class cybersecurity solutions to regional enterprises and we will never stop investing heavily in developing resources to identify the bleeding edge technologies, which are relevant for the regional enterprises.

As a distributor, our primary role is to scout for breakthrough technologies from across the globe and represent them in the region, so that businesses can enhance their cybersecurity postures and ultimately become more cyber-resilient.

What are the current issues channel partners are facing when it comes to effectively delivering cybersecurity

"AS A DISTRIBUTOR, OUR PRIMARY ROLE IS TO SCOUT FOR BREAKTHROUGH → TECHNOLOGIES FROM ACROSS THE GLOBE AND REPRESENT THEM IN THE REGION."

solutions? How are you enabling them to surpass these challenges?

Many channel partners face challenges in terms of having the right levels of expertise in-house to conduct PoCs and deployments. We are happy to announce that one of our solutions, Hive Pro, can overcome this challenge by automating and PoCs and deployments of several cyber security solutions at the customers end remotely. This helps speed up deployments and overcomes the challenges of limited expertise as well as current travel challenges.

What can we expect from Spectrami this 2020?

For Spectrami, it has been business as usual and in terms of revenue and we have managed to grow by 60 percent for this quarter as compared to the same quarter last year. We are running several marketing initiatives in association with our vendors and partners to spread awareness through online workshops and webinars.

Spectrami has more than 30 vendors in its portfolio and in past few months we have partnered with several industry leaders including Check Point, PhishRod, ColorTokens, Lookout, Wedge Networks, IntSights and Axonius, and we aim to continue supporting and fostering good relationships with them. **1**

HOW EUFY SECURITY BY ANKER CAN IMPROVE YOUR HOME SECURITY IN AN INSTANT

SYED SAMEER, SENIOR SALES & OPERATIONS MANAGER - EUFY SECURITY GCC, ANKER INNOVATIONS, DISCUSSES HOW THE COMPANY'S LATEST INNOVATIONS CAN KEEP HOMES SECURE AND SAFE.



or any household, the safety of every family member is paramount. That's why the concept of protecting one's home with a security system that can deter crime became accepted decades ago. Over the years, as smart home security solutions have evolved to become smarter and more connected. According to MarketsandMarkets, the smart home security system market is expected to reach \$74.75 billion by 2023, making it more apparent that such technologies are increasingly becoming an important feature in today's homes.

With home security more important than ever, eufyCam 2 from eufy Security by Anker brings a simple method for new and existing villa and apartment owners to set up their home security network. The system offers wire-free installation among other features to make monitoring your home a seamless and hassle-free process. eufyCam 2 offers 24 hours of security (No Monthly Fees) and with its advanced motion detection it sends you alerts anywhere you are, every time it detects movements. So, if you are leaving your children at home during work or you need a good night's sleep without worrying about anything, eufyCam 2 is for you and can trigger the alarm if an unwanted quest is at your front door

Suitable for any environment

Packaged with the device, users find everything to set up the security system in an instant. The Homebase 2 and eufyCam 2 are designed to suit any aesthetic with the latter also coming with full IP67 waterproofing and dust resistance. Given this, users can install the camera units both indoors and outdoors.

Privacy is also taken care of, with its military-grade encryption and local

Syed Sameer, Anker Innovations

storage, you can be assured that your personal data will always be safe.

Mountings required to place cameras also come out of the box. Users can take advantage of the versatility of the camera design too, either opting for a hardware screw mount or a strong magnetic mount based on preference and position. As for the Homebase 2, it doubles as an important productivity tool supporting Alexa and Google Assistant and encrypted local storage

Camera features

With the eufyCam 2's Sony STARVIS sensor, the camera is capable of recording and streaming Full HD footage even in low-light conditions. Furthermore, it brings support for features such as human detection, activity zones, two-way communication and smart image enhancement.

Artificial intelligence

It also gives you more flexibility by allowing you to set motion alerts according to your needs. For example, if you don't want to get an alert for when

> \$74.75 BILLION EXPECTED VALUE OF SMART HOME SECURITY SYSTEM

OME SECURITY SYSTEM MARKET BY 2023



pets or vehicles are detected outside your home you customise it like so. Following this, you can select to only receive notifications when people are detected outside your home.

All these features can be accessed via the free eufySecurity application, which provides instant notifications, live view and multi-user access. Best of all, there is provision for 16GB of free local storage with no other monthly fees or hidden costs.

One-year battery life

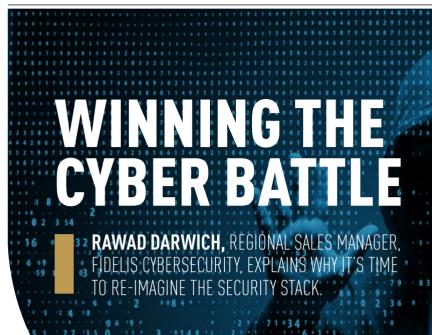
As impressive as the eufyCam 2 is, it also brings one year's worth of battery life on a single charge. This means users can be carefree about their surveillance system and can always rely on it.

The eufyCam 2 bundle comes with two cameras and a Homebase 2 unit to connect to your network, For anyone looking for a new home security system or a wire-free solution, this is the

ideal choice, you can buy at leading electronic retailers like Jumbo, Virgin, Sharaf DG, Emax, Danube Home, Lulu and online on noon.com and amazon.ae

eufy Security by Anker also has other products to complete your home security ecosystem with Video Doorbell, Floodlight Cam and soon to be launched Indoor Cameras..

INSIGHT



Rawad Darwich, Fidelis Cybersecurity

ata security is still the number one IT concern for businesses worldwide. A research carried out by ThoughtWorks in 2019 revealed that 33 percent of UK

business leaders said that 'data safety and cyber risk' was a bigger concern than the challenges of Brexit. Roll on six months and those concerns have increased exponentially as millions of people are now working from home due to the coronavirus pandemic. The story is the same for businesses in many countries across the globe and to address this, CIOs and CDOs are consistently 'adding' bolt-on security measures.

As new threats emerge, organisations add to their security stack by bolting on more cybersecurity tools. Combine the fact that many of the security 'solutions' are from different vendors with the problem of under-utilisation, not only are there a range of capabilities that are redundant but the organisation's entire security measures are complex and offer little to no benefits. Here's a fact from Fidelis Security's latest survey: less than seven percent of respondents were using their full security stack. Now that's a worrying statistic.

The negative impact of too many security layers

As technology advances, so does the threat level to businesses, which push them to be more reactive in dealing with the resulting cybersecurity issues. There has often been the situation whereby security tools have been implemented in order to address a specific problem with little thought as to how that integrates with existing systems. Fidelis found that some organisations have as many as 75 different cybersecurity tools in use, ranging from various firewalls and antivirus tools to intrusion detection and intrusion prevention tools, advanced threat protection tools and singlepurpose endpoint agent technologies.

In the drive towards digital transformation, magnified in recent months, this multi-layered Defense-inDepth approach has morphed into Defensein-Death as CIOs, CDOs and IT teams are discovering widespread under-utilisation. Couple that with a lack of automation and few cybersecurity professionals available, SOCs are struggling to deal with the influx of alerts from each and every cybersecurity tool, with many of those alerts having little or no context.

Ultimately, this reactive approach will impact response time but more worryingly, as the capabilities of each security tool overlaps with another, more layers of complexity are added resulting in little to no benefit in terms of overall security against cyber threats. Many businesses lack a comprehensive streamlined security infrastructure that provides real time visibility of their cyberattack surface, or little understanding of their critical asset vulnerabilities.

Re-thinking the security stack

Security stacks are overloaded; SOCs are dealing with an infrastructure that is fragmented and too complicated, leaving them **bo**uncing from one issue to another without the time and resources to identify the actual threat and resolving it successfully.

- Threat levels are rising, and changing in the new modern world. Businesses are facing several security challenges:
- A lack of real time visibility of their cyber-attack surface.
- A lack of automation of security systems and processes.
- Little or no threat intelligence tailored to the business.
- Few cybersecurity professionals' available, creating big skill gaps within the business.

Unmanageable, complicated, overcrowded security stacks that leave little time and resources to address modern-day cybersecurity threats.

Change is needed, and fast. This isn't lost on the security industry or businesses today. On the positive side, Fidelis Security's recent research demonstrated that there is

"WITH CONSOLIDATED SECURITY STACKS, THREAT HUNTERS ARE ABLE TO EFFECTIVELY IDENTIFY, ANALYSE AND RESOLVE UNKNOWN CYBER-THREATS."

a thirst for change with 78 percent of respondents admitting that they have, or are planning on, consolidating their security stack.

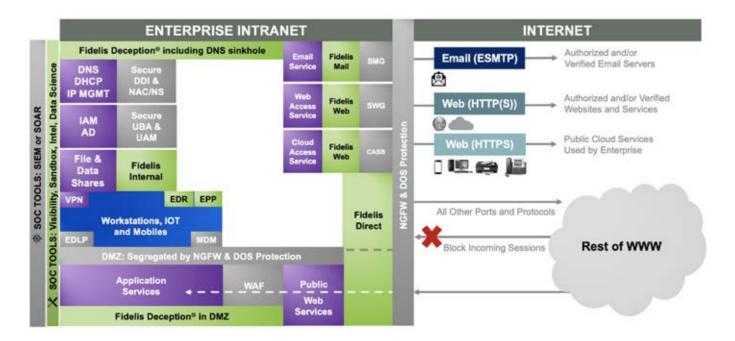
The security landscape has significantly changed, particularly in the last six months, and demand for unified security software solutions is high. Today, businesses are adopting automation capabilities to provide broader real time visibility into their networks and optimising digital workflows. But there is also a need to focus on people; given the right tools, people become threat hunters, discovering malware or suspicious activity that may be missed by other security solutions. With consolidated security stacks, threat hunters are able to effectively identify, analyse and resolve unknown cyber-threats.

Conclusion

By analysing and simplifying the existing cybersecurity stack, optimising their full capabilities in a focused, measured way, security professionals will be able to identify, manage and respond to the business's threat landscape effectively including:

- Addressing security methods and network endpoint visibility that detects and identifies internal and external threats.
- Securing the enterprise network perimeter, protecting internet access points and providing a network traffic analysis that records all activity.
- Managing cloud and web-based applications to streamline data traffic and secure workloads.

It's time to enable IT teams and SOCs with the right tools so they can do their job. The cyber battle will only be won through the consolidation of security stacks that deliver the right set of capabilities, enabling businesses to continuously detect, respond and protect their critical assets.



ENSURING BUSINESS CONTINUITY DURING A PANDEMIC

SECURITY CONSULTING FIRM CYBER RESILIENT GROUP'S FOUNDER **KAPIL MATTA** GIVES HIS TAKE ON WHY ORGANISATIONS NEED TO INCLUDE PREPARING FOR A PANDEMIC AS PART OF THEIR BUSINESS CONTINUITY PLANS

Kapil Matta, Cyber Resilient Group

usiness continuity planning is the process of creating a blueprint for dealing with challenging disasters, whether it be natural or man-made.

It ensures that an organisations can function close to business as usual without any disruption should any such event happens.

It involves everything from planning to conducting tabletop exercises and crisis management scenarios on ensuring key business products or services remain operational, recovery of important systems and technologies, people and processes mapped in case of disaster.

BCP as a practice is often implemented and tested in large enterprises or organization's – private and public, MNC's and government agencies. Since each business is unique, a comprehensive tailored BCP program is always advisable to best suit an organisation's operational requirements.

Usual BCP plans focus upon scenarios such as earthquake, act of war, vandalism, terrorist attacks and so on but usually not for a pandemic. Today, the global risk for catastrophe is not from nuclear attack but from biological attack or pandemic. Very few organisations undergo the pandemic scenario, the major reason being is that the rule of the land dictates that federal decisionmakers or government leadership should take control of the external situation.

An important aspect to remember is that in crisis scenario businesses

usually focus upon assets such as building, equipment and products. It is always considered that people will be available immediately after the crisis or the event has occurred. However, a pandemic – which involves an outbreak of an infectious disease – means employees would be unable to report back to work. Public health measures such schools, universities, social and religious gatherings among others will be limited or restricted depending on the severity of the situation.



From the what we have seen that during the WWI (Spanish Flu) where millions of people lost their lives across the globe to the recent Ebola outbreak, we still haven't learned our lessons. We were still unprepared to tackle such a catastrophic disaster at community, state or federal level. The key reason is that there is no system in place to test and measure such a scenario holistically from medical teams, and there is a lack of specialists such as epidemiologist to predict and control such an incident.

One of the key aspects for businesses need to ascertain in such a situation is to resonate the brand's responsibility towards its employees as well as its social and moral responsibility towards the society as a whole. Organisations need to focus on the essential business activities to exercise during the pandemic with limited staff or with rotation if possible. A planned and phased approach to start work immediately after recuperating from pandemic needs to be determined.

Here organisations need to have a people-centric approach towards continuity of their operation. Employees could be off work due to reasons:

- a. being quarantined or being sick themselves or their immediate family members being sick or quarantined during pandemic
- b. public health order by the state or federal authority
- c. volunteering role in-case of emergency declared by the federal authority
- d. worst case scenario such as death or disability due to infection by the virus

Hence, organisations need to include a remote working scheme as part of their business continuity plans. As we know by now, during a pandemic we cannot ascertain how much of our workforce will need to be function remotely and for how long.

To effectively implement a phased approach towards such a scenario, organisations – now matter smmal or large – need to conduct a business impact analysis or contingency plan to evaluate the potential impact of disruption to their business operations encompassing people, process and technology.

Organisations need to evaluate what is essential for their business to operate such as availability of personnel, assets, supplies, utilities, systems and most crucial data alongside incident response plans in case of emergencies. They also need to:

a. Identify and train people as back- ups for critical functions

- b. Identify critical machinery, services, applications systems, data etc and create a back-up of all those assets and availability to access them remotely
- c. Consider external factors such as availability of utilities such as power supply, water and so on
- d. Determine availability and dependency on third party vendors and suppliers – identify critical ones and their SLA's during emergencies
- e. Identify potential legal implications and business responsibilities to fulfil as an organisation towards clients and customers
- f. Prepare a call tree of all management or critical functions in case of emergency to take informed decision if anyone is unavailable for duty
- g. Secure the organisation's cash flows to ensure financing operations, payroll, invoicing and recovery
- h. Lastly, prepare an updated list of all emergency contact numbers of employees, hospitals, blood banks and government agencies.

An organisation's leadership team needs to be ready with the BCP strategy during a pandemic, if they have not then should follow the below mentioned brief process:

- 1. Assess
- 2. Design
- 3. Exercise
- 4. Maintain

Situations such as a pandemic need to have a dynamic approach by the key leadership team depending upon the situation. Organisations should follow above steps on an ongoing basis and need to assess their business operational situations daily and weekly, to make informed decisions.

WHY A PEOPLE-CENTRIC CYBER DEFENCE IS CRUCIAL

EMILE ABOU SALEH, REGIONAL DIRECTOR, MIDDLE EAST AND AFRICA, PROOFPOINT, DISCUSSES WHY UAE ENTERPRISES NEED A PEOPLE-CENTRIC APPROACH IN DEFENDING THEIR WORKFORCE AGAINST CYBER-ATTACKS.

ybercriminals are finding new and inventive ways to attack organisations in the UAE. Be it via Business Email Compromise (BEC), credential phishing or ransomware, attackers are increasingly chasing the same target our people rather than our infrastructure.

The people within our organisations not only make up a significant attack surface, but they are also viewed as more fallible than automated tools and technologies.

This is a view shared by a majority of CSOs and CISOs of UAE organisations. In fact, over half believe that human error and a lack of security awareness are the biggest risk factor facing their organisations. Emile Abou Saleh, Proofpoint

But while most CSOs and CISOs are aware of the risks and the consequences, many struggle to protect their business. Whether due to ineffective strategies, a lack of boardlevel concern or low levels of cybersecurity awareness, a change is needed – fast.

Adapting to a new approach

Defending against people-centric cyberattacks calls for a new approach. One that puts our people at its heart. To build and deploy such a strategy, we must first understand the type and frequency of attacks facing our organisations.

Over 80 percent of CSOs and CISOs in the UAE report suffering at least one cyber-attack in 2019, with over half reporting multiple incidents. It is, of course, people-centric attacks that top the list. Account compromise was reported by 28 percent of organisations,

reported by 28 percent of organisations, followed by credential phishing (20 percent), insider threats (17 percent), phishing (15 percent), and business email compromise (BEC) attacks (15 percent).

If the frequency of these attacks is not alarming enough, their success rates should cause grave concern. BEC accounted for estimated losses of \$1.7 billion last year while 55 percent of



organisations were victims of at least one successful phishing attack.

The consequences for the businesses behind these statistics can be farreaching – from lost revenues and reputational damage to downtime, legal fees, compensation, and remediation.

Only by understanding the type, frequency, and consequences of common attacks can we equip those on the frontline with the knowledge required to defend against them. Unfortunately, this is an area which, up to now, has been found wanting.

Despite the high stakes, most UAE organisations conduct security awareness training just once or twice a year – with only 2 percent implementing an ongoing

"BOARD LEVEL CYBER AWARENESS IS NOT ENOUGH. A PEOPLE-CENTRIC CYBER DEFENCE CAN ONLY BE EFFECTIVE WHEN IT IS COMPANY-WIDE."

education programme. This lack of continuous education is sadly reflected in employee awareness levels.

A recent Proofpoint study found that just two-thirds of the global workforce are familiar with the term phishing – with one in four having opened phishing emails and 10 percent admitting to clicking on malicious links within.

Against this backdrop, it's unsurprising that just 21 percent of CSOs and CISOs in the UAE strongly agree that their business is prepared for a cyber-attack. Evidently, while cyber risk and preparedness are on most organisations' agendas, the reality is often far from the desired state.

Turning awareness into action

Board level cyber awareness is not enough. A people-centric cyber defence can only be effective when it is companywide. Employees across all job levels and functions can put organisations at risk in numerous ways – as CSOs and CISOs know all too well.

Almost a third believe their employees make their business vulnerable to cyber attack through poor password hygiene, 25 percent through the mishandling of sensitive information, and 24 percent by falling victim to phishing attacks.

Unfortunately, there remains a clear disjunct between awareness of the problem and ability to implement a solution. This most likely stems from a lack of buy-in at board level – cited by 31 percent of CSOs and CISOs as a major obstacle to implementing effective cybersecurity measures.

Whether down to a lack of awareness, concern or understanding, this attitude has to change.

When our people come under attack, our people become our defence. We cannot expect them to saddle this enormous responsibility without first equipping them with the knowledge to do so. This means raising awareness of common attacks, and, most importantly, instilling an acute understanding of the end-user's role in defending against them.

Building a people-centric cyber defence

People-centric attacks call for a people-centric defence. Employees of all seniorities and job roles can be a target, so organisations must ensure that its entire workforce is equipped with the knowledge and the tools to defend against all manner of threats.

This is only achieved through company-wide training and awareness programmes. Training should be ongoing, comprehensive, and adaptive to the latest threats. As criminals continue to hone their attacks, so too must we continue to hone our defence.

As well as covering basics such as password hygiene and phishing detection, training should make clear the proven link between simple user behaviours and severe consequences.

Cybersecurity training has long been viewed as a compliance exercise – an attitude that leaves our organisations dangerously exposed.

You are not preparing your employees to pass a test. You are empowering them to protect your organisation from significant harm. Your training programme must reflect that.

CLOSING THE CYBERSECURITY GAP

AMMAR ENAYA, REGIONAL DIRECTOR – MIDDLE EAST, TURKEY & NORTH AFRICA (METNA), VECTRA, DISCUSSES THE BENEFITS OF MAKING DATA SCIENCE THE FOUNDATION OF NEW CYBERSECURITY MODELS.

Ammar Enaya, Vectra

known threats at scale. However, their

reductive - they reduce a known threat

weakness is that they are inherently

to its simplest fingerprint in order to

give a single yes or no answer within

microseconds to avoid slowing the flow

on immediate and simple answers has

created an advantage for attackers who

However, it is the persistence of the

attackers can blend in with the network,

progressively spy, and spread deeper,

steal or destroy. This process typically

involves multiple compromised hosts, a

until they find high-value assets to

ongoing attack that has truly turned

the tables. Once an organisation's

outer defences are compromised.

are willing to adapt.

of application traffic. This reductive focus

yber-attacks are no longer simple smash-and-grab jobs driven by pre-programmed malware. They are controlled by highly skilled, creative and intelligent humans. Ongoing coordination allows a human attacker to progressively learn more about the target network, adapt to any defensive measures, and advance the attack over time.

But while attacks have made an evolutionary leap in complexity, security defences have not. Signatures are the bedrock of traditional security technology and are written to identify exploits, malicious URLs and known malware as they seek to penetrate and gain an initial foothold inside the organisation. Signatures can quickly identify, and block variety of common tools and protocols that blend into the noise of everyday communications, and the theft and misuse of valid user credentials.

The important point is that the threat itself is ongoing while attackers evolve their operations and adapt over time. The reductive nature of signatures that identify threats at the atomic level is particularly ill-equipped for recognising the more complex chemistry going on around them. This intelligence gap is precisely why a new security model for threat detection is so vital.

Coarse-grained detections with a long shelf life

Detections that use traditional signatures become obsolete when attackers adapt by moving to a new domain or by adding a few bits to known malware, so signatures no longer match it. This gives them a first-mover advantage where even the most trivial changes keep attackers several steps ahead of defenders.

One of the core goals of the new threat detection model is to deliver detections that remain valid for long periods of time. This requires a shift from fingerprinting every individual instance of a threat to recognising the fundamental attack characteristics that every threat has in common. When applied to packetlevel traffic, data science and machine learning become extremely powerful tools to identify the fundamental characteristics that distinguish threats from normal traffic.

Focus on- attacker actions and behaviours

Traditional detection models attempt to find snippets of exploit code, a known sample of malware or a malicious domain. This leads to an intractable job of constantly finding and fingerprinting an infinite number of malicious occurrences. The task is never-ending, and attackers always remain steps ahead by using a new exploit.

To break this cycle, the new threat detection model shifts the focus from trying to name all possible bad 'things' to identifying the unique indicators of attack behaviours and actions. In other words, the goal shifts from identifying what a 'thing' is, to identifying what the 'thing' does. Although attackers can hide their threats by making slight changes to malware or buying a new domain, the actions and objectives of an attack are always the same.

By focusing on attack behaviours, defenders can fight and win the asymmetric cybersecurity war by shifting the math of

"BY FOCUSING ON ATTACK BEHAVIOURS, DEFENDERS CAN FIGHT AND WIN THE ASYMMETRIC CYBERSECURITY WAR BY SHIFTING THE MATH OF SECURITY BACK IN THEIR FAVOUR."

security back in their favour. Instead of using thousands of signatures to find every variant of a threat, they can focus on a few dozen key behaviours that attackers must perform in order to succeed.

Recognise threats over time

One of the most recognisable traits of modern network data breaches is that they evolve over time. This low-and-slow approach has become standard operating procedure for sophisticated attacks, and for good reason. Traditional security suffers from short-term memory and a post-breach form of perfect amnesia.

By understanding prevalent attacker Tactics, Techniques and Procedures (TTPs) from evidence-based sources like the Mitre ATT&CK framework, we can understand the steps that future possible attacks will use, and develop novel techniques to identify them.

The new threat detection model recognises threats in real-time and identifies the signs of attacks that evolve over time. One does not preclude the other. For example, small temporal anomalies and cadences within a network session can help reveal hidden tunnels and remote access tools used by attackers. Conversely, recognising when an employee's credentials have been compromised may require learning the user's normal behaviours over a period of days, weeks and months. While the time scale can vary, both cases require a keen understanding of threats in relation to time.

Recognise attacks, not just techniques

In order to provide value, security must identify real business risks to an organisation and not simply deliver a list of alerts. This requires security solutions to understand how individual events are interconnected and the impact those threats have on an organisation's assets. This necessitates a combination of threat context and organisational context. The ability to connect the dots between phases of an attack is precisely what distinguishes a targeted attack from the stream of commodity threats that inundate networks on a daily basis.

Why Data Science?

Data science represents a fundamental shift in security. Unlike a signature-based approach that delivers a 1-for-1 mapping of threats to countermeasures, data science uses the collective learning of all threats observed in the past to proactively identify new ones that haven't been seen before.

Long-term, it is essential to understand what, when, why and how. Actual knowledge and intelligence is far more advantageous when evaluating and solving new problems that have not been encountered before. This is a critically important distinction when using data science to detect threats. For the traditional model to work, all of the answers must be known ahead of time. Data science expects to be asked real questions and applies collective learning to evaluate an unknown.

As such, the newest, most advanced threat detection model combines a wide array of industry-leading intelligence and detection techniques to see threats from all angles in real time. It represents a new, more effective and highly proficient detection methodology that leverages data science to detect threats that are missed by traditional security models.

ARE YOU READY TO RESPOND TO A CYBER-ATTACK WHILE WORKING FROM HOME?

KAWTHER HACIANE, PROJECT EXECUTIVE AND SECURITY LEAD, IBM SECURITY SERVICES, HIGHLIGHTS WHY BUSINESSES NEED TO DOUBLE DOWN ON THEIR CYBERSECURITY EFFORTS AS THEY EMBRACE REMOTE WORKING MODELS.CYBER-ATTACK HOME.

Kawther Haciane, IBM Security Services

n 2019, the number of breached records jumped significantly with over 8.5 billion records exposed. According to IBM X-Force Threat Intelligence Index 2020, this is more than three times greater than 2018 year-over-year.

The increasing number of large-scale cyber-attacks suggests that not only is the rate of security breaches going up but increasing in severity, complexity and sophistication, and in turn, posing a significant threat to the reputation, brand value and financial situation of the affected organisations.

Over the past few weeks, more employees than ever have been working remotely from their homes. Every day, these employees are relying on Virtual Private Networks (VPNs) to access their organisations' data and information. And with that, cybersecurity issues are becoming tougher and a day-today struggle.

Although solutions, such as VPNs, are designed to make it easier to work remotely and collaborate, they open up tempting ways for hackers to get in. According to IBM X-Force, threat actors have plenty of choices on what to scan and exploit, with over 150,000 vulnerabilities publicly disclosed to date. It is, therefore, of high importance to update VPNs, network infrastructure devices and endpoints with the latest software patches and security configurations.

In addition to these basic cybersecurity hygiene practices, a multi-factor authentication (MFA) is no longer a "nice to have". As such, in 2019, according to the same IBM X-Force Threat Intelligence Index, unauthorised use of credentials, phishing and scan & exploit, were the overwhelming majority of the vector threat actors used to compromise security. Therefore, adopting an MFA solution is now a must for any company, regardless of its sise and can be one of the easiest and simplest ways to keep accounts protected.

Also, according to IBM X-Force spam collections, there is a significant spike in malicious activity and phishing campaigns to steal individuals' credentials.

It is essential for organisations to be transparent with their employees about the dangers of malicious activities, particularly those tempting individuals to click on links and become a victim of a phishing attack. And today, more than ever, companies must have an information



security awareness program in place, customised to take in consideration the work-from-home scenario.

In today's digitally disrupted world, organisations can no longer continue ignoring the likelihood of a breach to their environments. It is important that they acknowledge that it's not a matter of "if" you will experience a cybersecurity incident, but "when" and that when the inevitable occurs, almost every second counts and every action taken is critical.

Investing in a well-designed, pressuretested security incident plan will help organisations respond quickly and effectively to contain damage, minimise costs, and prevent reputational and business harm. And in the absence of such a plan, it is highly recommended to partner with a trusted external and specialised advisors in Incident Response, Forensics, threat intelligence and remediation services; to proactively prepare your cyber security response capabilities with their expertise, skills and resources. **1**

رقمیات Raqmiyat

System Integration. Digital Transformation. FORGING A FUTURE THAT CONNECTS IT ALL

The Future Of Smart Businesses

IT Consultancy | Enterprise Business & Digital Transformation | Cybersecurity | Next-Gen Infrastructure | IT Quality Assurance

The Next In Banking & OFinancial Services

Digital Banking | Enterprise Payment Hub | Payment Systems (Real-time & CBUAE) | Mobile Payments & Blockchain | Financial Peripherals |

The Tomorrow Of Technology Staffing

IT Professionals Outsourcing | Managed Services | Infrastructure & Datacenter Management | Helpdesk/End User Support | Network & Security Management

UAE | KSA | India

www.raqmiyat.com



SMART ACCESS FOR SECURE CONTROL



SECNOR ACCESS CONTROL SYSTEM

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

NORDEN[®]



Norden Communication UK Ltd

Unit 13, Baker Close, Oakwood Business Park, Clacton-on-Sea, Essex, CO15 4BD, United Kingdom Tel: +44 [0] 1255 474063, E-mail: support@norden.co.uk, Web: www.norden.co.uk www.nordencommunication.com