

Security

ADVISOR

MIDDLE EAST

FEATURE

THE DECISION
DILEMMA

SPECIAL
REPORT
PROTIVITI

INTERVIEWS

HIKVISION
D-LINK
RING

CLOSING

JAMES LYNE, CHIEF TECHNOLOGY OFFICER, SANS INSTITUTE, TELLS SECURITY ADVISOR HOW CYBERSECURITY SPECIALISTS WITHOUT BASIC IT SKILLS ARE LIKE SURGEONS THAT DON'T KNOW ANATOMY.

THE SKILLS GAP



ENJOY SAFER TECHNOLOGY™

YOUR DATA IS YOUR BUSINESS



ENDPOINT
SECURITY



DATA
ENCRYPTION



SECURE
AUTHENTICATION



DETECTION &
RESPONSE



CLOUD
SANDBOXING



MAIL
SECURITY

**MAKE SURE YOUR COMPANY
IS SAFE FROM DATA BREACHES
OR LEAKS. EMPLOY OUR
POWERFUL AND EASY TO DEPLOY
ESET SECURITY SOLUTIONS.**

110m+

users worldwide

400k+

business customers

200+

countries & territories

13

global R&D centers

WWW.ESET.COM/ME

CONTENTS



06 **NEWS**
News round-up from the world of cybersecurity

INTERVIEW

12 Binson Xu, president MENA region at Hikvision, on how the company's 'Secure-by-design' philosophy ensures that security is built into every stage of its product production process- right from the idea-to final production and delivery.

22 Werno Gevers, regional manager at Mimecast Middle East, on the strides AI is making in cybersecurity

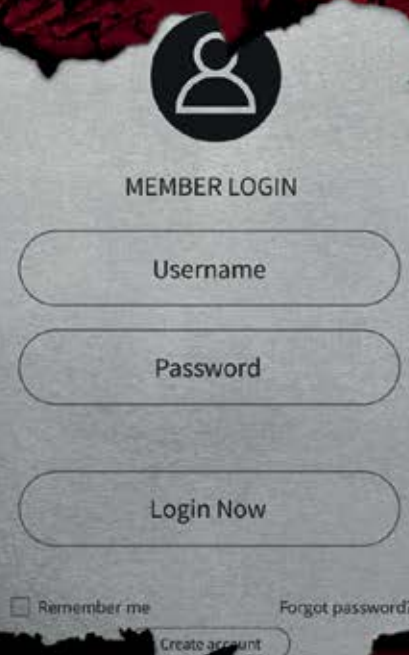
and how the company is leveraging this technology to provide intelligent cybersecurity solutions.

30 Protiviti Member Firm for the Middle East Region, a global business consulting firm, on how they help businesses address challenges and opportunities in key areas such as technology, digital transformation, business process improvement, risk management, compliance, transaction advisory and internal audit.

50 Dev Mehta, director, International Marketing at Virsec, on what makes up his world.

mimecast®

The State of Brand Protection 2021



MEMBER LOGIN

Username

Password

Login Now

☐ Remember me [Forgot password?](#)

[Create account](#)

A new front opens up in the war of brand safety

Did you know that **40%** of consumers don't hesitate to click on links in emails from their favorite brands?

Download our **State of Brand Protection** report to become the master of your brand domain and learn how to keep your brand safe from #cybersecurity threats.



www.mimecast.com/state-of-brand-protection

NASDAQ: MIME

EDITORIAL



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

Anita Joseph
Editor

THE CHANGING SECURITY LANDSCAPE

The role of the CISO50 is becoming more important today than it has ever been. 2021 being the year of rapid transformation and recovery from the impact of the pandemic, the conversation around security is front and center. So much so that it's become top priority for business leaders as the world prepares to recover from the damages of 2020. This puts the Chief Information Security Officer and other security professionals in the hot seat — from the weekly IT department stand-up to the quarterly board meetings. What are the challenges that they face as they steer their companies through uncertain times? What is their strategy for success? This is the conversation that no business can afford to miss today.

This crucial topic is what we have

focused on in this issue—the challenges that security decision makers have to face as they navigate an increasingly complex threat and security landscape. We speak to some of the who's-who in the security world to find out what they think.

THE ROLE OF THE
CISO AND IT
DECISION MAKER
IS CHANGING.

In addition to this, we have special interviews with Hikvision, D-Link, Mimecast, ManageEngine and Ring, about the changing face of security technology. Our cover story is with SANS Institute,

about closing the skills gap in the world of cybersecurity. In addition, we also have the regular news updates and in-depth reports about security and its ramifications.

This is an engrossing issue—one which we're sure you won't be able to put down. So, happy reading!

EVENTS



FOUNDER, CPI MEDIA GROUP
Dominic De Sousa (1959-2015)

Published by
CPI

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

**EDITORIAL
Editor**
Anita Joseph
anita.joseph@cpimediagroup.com

**DESIGN
Senior Designer**
Analou Balbero
analou.balbero@cpimediagroup.com

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

**ADVERTISING
Group Sales Director**
Kausar Syed
kausar.syed@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

**DIGITAL SERVICES
Web Developer**
Adarsh Snehanjan

Reception: +971 4 5682993
Operations: +971 4 5682994
Accounts: +971 4 5682995

Senior Sales Manager
Sabita Miranda
sabita.miranda@cpimediagroup.com

© Copyright 2021 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.

SANS INSTITUTE INTRODUCES #SECURETHEFAMILY CAMPAIGN TO HELP PROTECT FAMILIES ONLINE

HEATHER MAHALIK



This October, for

Cybersecurity Awareness Month, SANS Institute [SANS] is encouraging everyone to spread security awareness programs beyond the boundaries of the office and to help all employees and co-workers apply the lessons learned at work to protect their families and friends with the global #SecureTheFamily initiative.

Today, we are more digitally connected than ever before, as more people work from home, remote e-learning has grown exponentially, and Wi-Fi-enabled "smart" devices increasingly occupy different aspects of our daily lives. Connected personal assistant devices can control your smart home devices, digital refrigerators can track your food inventory, video monitors allow you to keep an eye on your little one anywhere from your smartphone, thermostats and light bulbs can connect to your home Wi-Fi, and some washing machines let you remotely schedule wash cycles in advance. All of this connectivity brings plenty of benefits and convenience, but each connected device also brings increased risk.

"Every personal device used is a potential entry for system threats," said Heather Mahalik, digital forensics expert, SANS faculty fellow, Cellebrite senior director of Digital Intelligence and mother of two. "Cyber attackers can target anyone's home – no one is invulnerable. Risks to our digital safety are everywhere, but there are steps you can take to protect yourself and your family."

Mahalik developed the SANS Security Awareness curriculum for #SecureTheFamily with practical advice on securing personal devices and data and how to keep families safe online.

THREATQUOTIENT PUBLISHES STATE OF CYBER SECURITY AUTOMATION ADOPTION RESEARCH REPORT FOR 2021

ThreatQuotient, a leading security operations platform innovator, has released the State of Cyber Security Automation Adoption in 2021—a new research focused on understanding the importance, challenges and trends facing businesses when it comes to automating their IT security systems. The report determined that 98% intend to automate more in the next 12 months, but 41% have a lack of trust in automation's outcomes.

The State of Cyber Security Automation Adoption in 2021 report surveyed five key vertical markets: Central Government, Defense, Critical National Infrastructure – Energy and Utilities, Retail and Financial Services. The research examines what IT security use cases or processes organisations have already automated and what they are planning to automate, as well as budgets, skills, resources, issues around trust, and assesses the overall outlook for IT security automation.

ANTHONY PERRIDGE



"To gain a clearer picture of the state of IT security automation and adoption, and understand what is either accelerating or holding UK PLC back, we commissioned this survey to understand how far down the road senior cybersecurity professionals are with their IT security automation initiatives," said Anthony Perridge, vice-president, International, ThreatQuotient. "There are several barriers preventing organisations from maximising the benefit of automation, such as budget, prioritisation issues, talent gaps, technology, trust concerns and more. At ThreatQuotient, we know that data driven automation can enable security operations teams to reliably trust the data and be confident in their decisions, which for many security professionals will be absolutely ground-breaking as they look to automate more use cases."

MCAFFEE ENTERPRISE SEES PROLIFERATION OF REVIL AND DARKSIDE RANSOMWARE SURGE IN Q2 2021

McAfee Enterprise has released its Advanced

Threat Research Report: October 2021, examining cybercriminal activity related to ransomware and cloud threats in the second quarter of 2021. With the shift to a more flexible pandemic workforce and the highly publicised Colonial Pipeline attack, cyber criminals introduced new – and updated – threats and tactics in campaigns targeting prominent sectors, such as government, financial services and entertainment.

"Ransomware has evolved far beyond its origins, and cybercriminals have become smarter and quicker to pivot their tactics alongside a whole host of new bad-actor schemes, said Raj Samani, McAfee Enterprise fellow and chief scientist. "Names

RAJ SAMANI



such as REvil, Ryuk, Babuk, and DarkSide have permeated into public consciousness, linked to disruptions of critical services worldwide. And with good measure, since the cybercriminals behind these groups, as well as others, have been successful at extorting millions of dollars for their personal gain."

Each quarter, McAfee assesses the state of the cyber threat landscape based on in-depth research, investigative analysis, and threat data gathered by the McAfee Global Threat Intelligence cloud from over a billion sensors across multiple threat vectors around the world.

SOPHOS ACCELERATES GROWTH OF MSP CONNECT

Sophos, a global leader in next-generation cybersecurity, has announced accelerated worldwide growth of MSP Connect, Sophos' award-winning program to help managed service providers (MSPs) increase customer management efficiencies, unlock new business opportunities and boost revenue. The growth is fueled by the increased demand for Sophos' next-generation cybersecurity solutions and services that protect against ransomware and other cyberthreats.

Sophos MSP Connect achieved 67% year-over-year billings growth in the first quarter fiscal year 2022, ending June 30, 2021, and 55% year-over-year billings growth in fiscal year 2021, ending March 31, 2021, through MSP Connect Flex, Sophos' flexible monthly billing program. MSP Connect now supports more than 16,500 global and regional MSPs worldwide, a 54% increase since April 1, 2020, the start of Sophos' fiscal year 2021.

SCOTT BARLOW

"The world experienced a necessary shift to remote working this past year, requiring businesses to rely heavily on the cloud. MSPs have been on the frontlines since day one, helping organisations secure hybrid workforces with remote employees – a critical role considering changing attacker tactics, techniques and procedures (TTPs) that increasingly involve remote access services such as Remote Desktop Protocol (RDP)," said Scott Barlow, Sophos vice-president of global MSP and cloud alliances. "MSP Connect makes it easier than ever for MSPs to secure diverse customer environments with one comprehensive cybersecurity portfolio that's simple to deploy and manage."



SANS INSTITUTE ANNOUNCES TRAINING PROGRAM TO NARROW CYBERSECURITY SKILLS GAP IN GCC

SANS Institute, the global leader in cybersecurity training and certifications, has announced its upcoming online and in-person training program, SANS Gulf Region 2021, to be hosted from 6th – 25th November, 2021. The interactive event, led by industry experts, aims to build practical skills that participants can put into immediate effect. The program includes nine courses covering an extensive and immersive range of cybersecurity tactics. From standardised foundational skills, detecting and responding to threats, assessing deficiencies in an organisation's security architectures, to conducting successful penetration testing and ethical hacking projects, SANS Gulf Region 2021 offers a comprehensive training experience.

"Synchronous with the acceleration in remote work due to the pandemic, the cyber threat landscape is rapidly

NED BALTAGI

evolving in the GCC region. Consequently, the need for relevant and updated security increases as cybercriminals take advantage of this ongoing shift to execute attacks on vulnerable networks. By participating in and implementing learnings from regular training programs like SANS Gulf Region 2021, organisations will be better prepared to detect and prevent security breaches, even before they can escalate and disrupt workflow," said Ned Baltagi, managing director – Middle East and Africa at SANS Institute.

In the latest threat intelligence report released by Check Point Software Technologies Ltd, it was revealed that organisations in the UAE alone have experienced at least one intrusion and on average, been targeted for attack 295 times per week in the last six months.



BARRACUDA TO SHOWCASE HOW MIDDLE EAST BUSINESSES CAN SECURELY EMBRACE CLOUD AT GITEX 2021

CHRIS ROSS



This year, Barracuda, a trusted partner and leading provider of cloud-enabled security solutions, will return to GITEX with a full range of cybersecurity solutions that enable businesses to secure their mission-critical applications and data in a digitally transformed world. The company's technology focus will be on its Cloud Application Protection solution which provides powerful application security that is easy to use and helps protect applications deployed on-premises, in the cloud, or hybrid. Barracuda is also set to unveil expanded incident response capabilities for its Total Email Protection offering, a suite of powerful security solutions that offer protection against a wide range of email threats.

"While packed with powerful features, Barracuda's enterprise-grade security solutions offer consumer-level ease of use, enabling organisations to focus on realising their digital ambitions with confidence in the security of their digital services and assets," said Chris Ross, SVP International Sales, Barracuda Networks.

In its latest report Barracuda found that 72% of organisations got breached through web applications. Moreover, the causes of these attacks varied, with top threats including bad bots (43%), software supply chain attacks (39%), vulnerability detection (38%), and securing APIs (37%). By leveraging machine learning, vulnerability scanning and remediation and Advanced Threat Protection, Barracuda Cloud Application Protection provides active threat intelligence for protection against these and other application threat vectors.

ESET RESEARCH UNCOVERS TARGETED MALWARE ATTACKING LINUX IN SOUTHEAST ASIA



ESET researchers have discovered a previously unknown malware family that utilises custom and well-designed modules, targeting operating systems running Linux. Modules used by this malware family, which ESET dubbed FontOnLake, are constantly under development and provide remote access to the operators, collect credentials, and serve as a proxy server. The location of the C&C server and the countries from which the samples were uploaded to VirusTotal might indicate that its targets include Southeast Asia.

“The sneaky nature of FontOnLake’s tools in combination with advanced design and low prevalence suggest that they are used in targeted attacks,” said Vladislav Hrčka, ESET malware researcher who analysed this threat. To collect data or conduct other malicious activity, this malware family uses modified legitimate binaries that are adjusted to load further components. In fact, to conceal its existence, FontOnLake’s presence is always accompanied by a rootkit. These binaries are commonly used on Linux systems and can additionally serve as a persistence mechanism.

ESET researchers believe that FontOnLake’s operators are overly cautious since almost all samples seen by ESET use different, unique C&C servers with varying non-standard ports. The authors use mostly C/C++ and various third-party libraries such as Boost, Poco and Protobuf.

The first known file of this malware family appeared on VirusTotal last May and other samples were uploaded throughout the year. None of the C&C servers used in samples uploaded to VirusTotal were active at the time of writing, indicating that they could have been disabled due to the upload.

KASPERSKY DISCOVERS ADVANCED STEALER THAT TARGETS ACCOUNTS OF ONLINE GAMING PLATFORMS



Kaspersky researchers have discovered

an advanced Trojan, dubbed the BloodyStealer, sold on darknet forums and used to steal gamers’ accounts on popular gaming platforms such as Steam, Epic Games Store, and EA Origin. With features to avoid analysis and detection, a low subscription price, and some interesting capabilities, BloodyStealer is a prime example of the type of threat online gamers face. This, alongside an overview of the game-related products stolen and sold on the darknet, can be found in Kaspersky’s latest report on game-related data threats. As demonstrated in the latest Kaspersky research, in-game goods and gaming accounts are in demand on the darknet. Combinations of gaming logins and passwords to popular platforms such as Steam, Origin, Ubisoft or EpicGames can sell as cheaply as 14.2 USD per thousand accounts when sold

in bulk, and for 1-30% of an account’s value when sold individually. These stolen accounts do not come from accidental data leaks, but are the result of deliberate cybercriminal campaigns that employ malware such as BloodyStealer.

BloodyStealer is a Trojan-stealer capable of gathering and exfiltrating various types of data, for cookies, passwords, forms, banking cards from browsers, screenshots, log-in memory, and sessions from various applications. These include gaming ones – EpicGames, Origin, and Steam in particular. This malware also stands out to researchers because of several anti-analysis methods used to complicate its reverse engineering and analysis, including the use of packers and anti-debugging techniques.

UAE RESEARCHERS IMPROVE FEASIBILITY OF ALGORITHMS TO STRENGTHEN BLOCKCHAIN SECURITY

Researchers at Technology Innovation

Institute (TII) in the United Arab Emirates have improved the feasibility of a new class of algorithms to protect blockchain applications against quantum computing cryptographic attacks. This builds on the considerable research already underway across the cryptographic community in developing better protocols for improving zero-knowledge proofs.

The specialised area of cryptography has been gaining significant interest since zero-knowledge proofs are widely used in techniques like blockchain, smart contracts, and identity verification.

The most popular approaches have involved using matrix computations. However, there is some concern that future research may find new and improved ways to compromise these protocols. So, researchers are always looking



for promising alternatives to provide multiple types of protection against future cryptographic attacks.

The various types of quantum-resistant problems and algorithms built on them are considered safe at the present time, because no one has demonstrated a credible quantum computer attack against them. Emanuele Bellini, lead cryptographer at TII, said: “We are in the early stages of understanding what is quantum-resistant and what is not. The safest approach is to build the quantum-resistant scheme based on many different problems so that if one is broken, you are still hopeful that the others are not.”



Russia has a powerful cybersecurity industry.
We are No.1 in strong authentication, electronic signature
and software protection domains.

Create a secure cryptographic environment
at the state level for the exchange of essential
information.

1

Strong
authentication
and electronic
signature

2

Software monetization
and protection against
reverse-engineering

3

Consulting
and training
in cybersecurity

Be sure you are protected



Technologies for a secure future



aktiv-company.com



global.guardant.com



BEYONDTRUST REMOTE SUPPORT NOW INTEGRATES WITH MICROSOFT TEAMS

BeyondTrust, the worldwide leader

in Privileged Access Management (PAM), has announced BeyondTrust Remote Support 21.3, featuring a new integration with Microsoft Teams. Users can now chat via Teams directly with a support representative using BeyondTrust Remote Support and, if needed, elevate to a fully audited remote screen sharing session without ever leaving Microsoft Teams. "Support teams need a simplified, seamless and intuitive interface for their end users to gain access to the support they need," said Tal Guest, director of Product Management at BeyondTrust. "These key integrations with Microsoft will allow organisations to streamline their end user experience and better secure their enterprise environments."

TAL GUEST

IT service desks face an increasingly complex support environment.

Many organisations continue to use a combination of remote access products, including free tools, that cannot scale across their enterprise and lack the security features required to protect the organisation from modern cyberattacks.

BeyondTrust Remote Support gives organisations the capability to support a wide range of devices, including unattended systems and IoT, while increasing operational efficiency, and lowering downtime and costs.



CYBEREASON EXPOSES CYBER ESPIONAGE CAMPAIGN TARGETING GLOBAL AEROSPACE & TELECOMMUNICATIONS FIRMS

Cybereason, the leader in operation-centric attack protection, has published a new threat intelligence report that unmasks a highly-targeted cyber espionage operation targeting global aerospace and telecommunications companies.

The report identifies a newly discovered Iranian threat actor behind the attacks dubbed MalKamak that has been operating since at least 2018 and remained unknown until today.

In addition, the still-active campaign leverages a very sophisticated and previously undiscovered Remote Access Trojan (RAT) dubbed ShellClient that evades antivirus tools and other security apparatus and abuses the public cloud service Dropbox for command and control (C2).

The report details the stealthy attacks against companies in the

LIOR DIV

Middle East, United States, Europe and Russia. The investigation reveals possible connections to several Iranian state-sponsored threat actors including Chafer APT (APT39) and Agrius APT.

Lior Div, Cybereason CEO and co-founder, said: "Layering on more tools to produce even more alerts that overwhelm defenders is not helping us stop sophisticated attacks, which is why Cybereason takes an operation-centric approach that detects based on very subtle chains of behavior where the adversary's own actions work against them to reveal the attack at the earliest stages."



TWO-THIRDS OF ORGANISATIONS HAVE BEEN TARGET OF AT LEAST ONE RANSOMWARE ATTACK, SAYS FORTINET SURVEY

JOHN MADDISON



Fortinet, a global leader

in broad, integrated, and automated cybersecurity solutions, has unveiled the 2021 Global State of Ransomware Report. The survey reveals most organisations are more concerned about ransomware than other cyberthreats. However, while the majority of organisations surveyed indicated they are prepared for a ransomware attack, including employee cyber training, risk assessment plans, and cybersecurity insurance, there was a clear gap in what many respondents viewed as essential technology solutions for protection and the technology that can best guard against the most commonly reported methods to gain entry to their networks.

John Maddison, EVP of Products and CMO at Fortinet, said: "According to a recent FortiGuard Labs Global Threat Landscape report, ransomware grew 1070% year over year. Unsurprisingly, organisations cited the evolving threat landscape as one of the top challenges in preventing ransomware attacks. As evidenced by our ransomware survey, there is a huge opportunity for the adoption of technology solutions like segmentation, SD-WAN, ZTNA, as well as SEG and EDR, to help protect against the threat of ransomware and the methods of access most commonly reported by respondents."

"The high amount of attacks demonstrates the urgency for organisations to ensure their security addresses the latest ransomware attack techniques across networks, endpoints, and clouds. The good news is that organisations are recognising the value of a platform approach to ransomware defence," he added.

Accelerating Sustainable Digital Transformation

At Moro Hub, we promise to deliver value by leveraging our expertise, capabilities and alliances to contribute to successful digital transformation journey.



Digital Solutions



Cloud & Hosting Services



Professional & Managed Services



Smart Cities & IoT Services



Cyber Security Services



A NEW APPROACH TO SECURITY

BINSON XU, PRESIDENT MENA REGION AT HIKVISION, TELLS SECURITY ME HOW THE COMPANY'S 'SECURE-BY-DESIGN' PHILOSOPHY ENSURES THAT SECURITY IS BUILT INTO EVERY STAGE OF ITS PRODUCT PRODUCTION PROCESS- RIGHT FROM THE IDEA-TO FINAL PRODUCTION AND DELIVERY.

How would you describe the video security market in the region, especially post-pandemic?

At the beginning of the pandemic, the demand for video security equipment decreased significantly for some time. However, as the world and the region recovered, the market returned to growth with an overall demand higher than pre-COVID times. People began to care even more about their personal safety and in their communities. There was also an upsurge in demand from online businesses for remote monitoring solutions and services. So, in short, the video security business is doing very well right now.

What has Hikvision's strategy been, for growth and diversification in the market?

We normally divide the business into

channel business and project business. As far as the channel business is concerned, we always keep improving our channel coverage to make sure that all our customers can get easy access to our products and services. This is a key element of our strategy. For the project business, our main objective is to provide solutions to our customers across different verticals, to make sure they can really meet their business requirements and expectations. This is also a key strategic focus area for us. During the pandemic, we changed all of our sales and marketing services and facilities from offline to online/offline, to ensure the best possible response time and efficient support for our customers.

How does Hikvision ensure the security of its products?

First of all, Hikvision has implemented 'Secure-by-design', which is a cybersecurity philosophy or approach



Binson Xu

“HIKVISION HAS ITS OWN CYBER LABS TO MAKE SURE ALL OF OUR HARDWARE AND SOFTWARE ARE CERTIFIED AND QUALITY-CHECKED AND ADHERE TO THE MOST RIGOROUS INTERNATIONAL CERTIFICATION STANDARDS.”

that aims to bake security into every stage of a product's production process. It begins at the conceptual phase when a video camera or other product is still on the drawing board, and it extends through development and testing, right through to final production and delivery.

Hikvision has its own cyber labs to make sure all of our hardware and software are certified and quality-checked and adhere to the most rigorous international certification standards. We follow all standard protocols and APIs and upgrade our firmware and software regularly to make sure we can improve and enhance our products as per market requirements. This is basically what we do, to make sure our products are safe and secure for use.

What is Hikvision's plan for the regional market in the coming years?

Again, for the region, we have divided our business by channels and projects. In the channel, we have already achieved good coverage to support our customers effectively, and now we would like to provide a one-stop-shop solution for all partners, so that they can benefit from access to a wider range of products from Hikvision. For the project business, we can see that the trends shaping the market right now are digitalisation and Artificial Intelligence (AI) and that the demand for cloud and IoT are also ramping up. Our goal is to provide vertical solutions matching those opportunities and the fundamental needs of our end-users to protect people and assets, while also improving operational efficiency to help make their businesses more profitable. So that's going to be our strategy and focus for the region. 📌

RELATIONSHIP BETWEEN SECURITY, IT & DEVELOPERS MUST IMPROVE TO DRIVE INNOVATION: VMWARE

TECHNOLOGY TEAMS REQUIRE ALIGNMENT WITH COMMON GOALS FOR A STRONG SECURITY POSTURE AND FAST APPLICATION DELIVERY, SAYS VMWARE'S STUDY ON THE RELATIONSHIP BETWEEN IT, SECURITY, AND DEVELOPMENT TEAMS.

Ahmed El Saadi

Innovating at pace to create exceptional customer experiences is increasingly setting companies apart, but the technology teams responsible for this – security, IT and developers – must be aligned to these goals to deliver this. However, security is still perceived as a barrier in organisations, with 61% of IT teams and 52% of developers believing that security policies are stifling their innovation. These are the latest findings from VMware, Inc.'s study on the relationship between IT, security, and development teams.

The study, titled "Bridging the Developer and Security Divide" and conducted by Forrester Consulting surveyed 1,475 IT and security leaders and discovered that only one in five (22%) developers strongly agree that they understand which security policies they are expected to comply with. Alarming, more than a quarter (27%) of those surveyed are not involved at all in security policy decisions, despite many of these greatly impacting their roles. Organisations where security and development teams have a positive relationship can accelerate the software development lifecycle five business days faster than those without – demonstrating how speed to market and competitive advantage are at stake here.

The findings reflect that team priorities are not always aligned to customers, with IT and security teams rating their number one priority as operational efficiency (52%) versus developers whose priority is improving the user experience (50%). Meanwhile, improving the user experience ranks fourth for IT (43%) and security (40%). More than half (51%) of security teams cite preventing security breaches as their second priority. These teams that are struggling to align have found themselves with increased silos and decreased collaboration across teams (60%), an increased risk of security breaches (57%) and a slower release of new applications (40%).

"Our research shows that security needs a perception shift," said Rick McElroy, principal cybersecurity strategist at VMware. "Rather than be seen as the team that only swoops in to fix breaches and leaks, or who 'gets in the way' of innovation, security should be embedded across people, processes, and technologies. Security needs to be a team sport that works alongside IT and developers to ensure protection across clouds, apps and all digital infrastructure. We have to develop a culture where all teams have shared interests and common goals or metrics, and where they speak one language. There's overwhelming

value to the business when IT, security, and developers are all part of the decision making, design, and execution."

The good news is there is recognition that shared team priorities and engagement is the way forward. More than half (53%) of respondents expect security and development teams to be unified two-three years from now. 42% expect security to become more embedded in the development process in two-three years' time, and there's a broader acknowledgment that cross-team alignment empowers businesses to reduce team silos (71%), create more secure applications (70%) and increase agility to adopt new workflows & technologies (66%).

"The findings of the research fit closely with what we see in the Middle East and North Africa," said Ahmed El Saadi, Regional Director of Sales, Middle East, Turkey, Africa, VMware. "For many organisations, a lack of collaboration between IT, security and development teams leads to challenges that slow development and hinder security. It's imperative that teams adopt a collaborative approach from the outset, pull in the same direction, and ensure that security is embraced as an intrinsic part of their IT and development procedures." 🧑

Computers, Technology and Security

SANS Foundations is the best single course available to learn core knowledge and develop practical skills in computers, technology, and security fundamentals that are needed to kickstart a career in cybersecurity.

What is included with SANS Foundations?

- Over 120 hours of curated content
- Hands-on labs experience
- Quizzes to consolidate learning outcomes
- Training by world-renowned experts
- Engaging 4K video content
- Proctored final exam delivered by GIAC

What will Students learn in this course?

The course provides students with exactly what they need to go from zero technical and security knowledge to a level of sufficient theoretical understanding and applied practical skills that will enable them to speak the same language as industry professionals. Students will develop fundamental skills and knowledge in key IT subject areas such as Linux, programming, networking, computer hardware, operating systems, encryption, basic security concepts, and more!

Who should take this course?

This course is designed for:

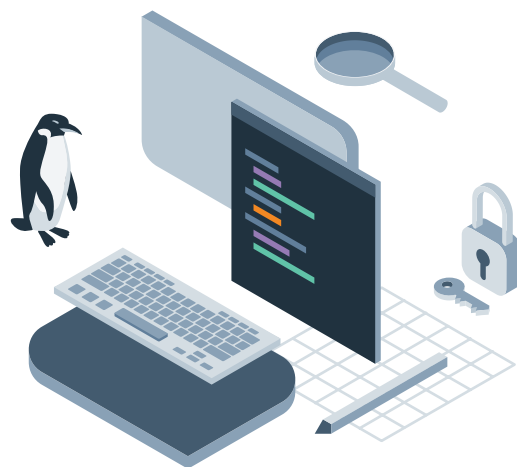
- Career changers
- Online self-driven learners seeking new skills
- College and university students
- Business professionals without a deep cybersecurity background
- New hires in IT/cybersecurity
- Participants in reskilling programs

For more information visit

sans.org/close-skills-gap

or email

foundations@sans.org



I think the biggest value add for SANS Foundations was simply how comprehensive it was. It covered a lot of topics, but each was covered in enough depth for a better handle on the basics without being overwhelming.

- U.S. government federal law enforcement professional

CLOSING THE SKILLS GAP

JAMES LYNE, CHIEF TECHNOLOGY OFFICER, SANS INSTITUTE, TELLS SECURITY ADVISOR HOW CYBERSECURITY SPECIALISTS WITHOUT BASIC IT SKILLS ARE LIKE SURGEONS THAT DON'T KNOW ANATOMY.

“AT SANS WE HAVE BEEN TRAINING PEOPLE IN CYBERSECURITY FOR YEARS. THESE ARE PEOPLE WHO COME TO REFRESH THEIR KNOWLEDGE, TO LEARN NEW CYBERSECURITY SKILLS, BUT ALSO PEOPLE WHO ARE NEW TO THE INDUSTRY.”

There is a serious shortage of cybersecurity specialists the world over. In fact, studies show that almost 70% of cybersecurity professionals the world over claim that their organization is impacted by a lack of cybersecurity skills. What this means for the industry as a whole is increased workload on existing security & IT staff; open, unfilled vacancies, hiring of random junior professionals and an inability to utilise technology to its full potential.

Those in the industry say that skills shortage is most acute

among security analysts and cloud security professionals. And with more organizations accelerating their digital transformation journey and shifting entire workspaces to the cloud, this shortage becomes a matter of grave concern.

Again, the cybersecurity skills gap has two sides to it: the first is that there aren't enough cybersecurity professionals and two, there aren't enough professionals skilled in dealing with the new and emerging demands of cybersecurity.

In order to address the skills gap, SANS Institute offers training at various levels. What this means is that not only can seasoned cybersecurity experts increase their knowledge, but people who are new to the industry can also build a solid foundation for a career in cybersecurity. Core knowledge and practical skills in computers, technology and security fundamentals are crucial for launching a career. That's why SANS developed its' new SANS Foundations course.

"At SANS we have been training people in cybersecurity for years. These are people who come to refresh their knowledge, to learn new cybersecurity skills, but also people who are new to the industry." The training organization



SANS Foundations

LEARN THE FUNDAMENTALS

Gain real-world skills and knowledge from the top experts in cybersecurity. The SANS New To Cybersecurity curriculum features multiple options to meet the needs of anyone looking to enter the field. From zero technical experience to basic IT knowledge, SANS has a solution that will enable you to select a starting point for your cybersecurity learning journey.

SEC275: Foundations - Computers, Technology & Security

This is the best course to help people with no technical experience understand the concepts of computers, technology and cybersecurity. Take a course walk through and see what this course has to offer.

SEC301: Intro to Cybersecurity

This course offers a balanced mix of technical and managerial issues for students who need to understand the salient facets of basic information security and risk management.

SEC401: Security Essentials: Network, Endpoint, and Cloud

Learn essential information security skills and techniques to protect and secure critical information and technology assets. This course dives deep into active defense, cryptography, networking, architecture, Linux, security policy, Windows, web security, Cloud and much more!



saw across the globe that, especially for these newbie's, it is not always easy to understand the fundamentals of cybersecurity. "This is because they lack some basic concepts of computers, networks, data or applications. And those very elements are crucial to understanding how cybersecurity works." Lyne draws the comparison with a surgeon. "Basically, we were training cardiologists without them knowing any anatomy. That's a frightening idea, isn't it? That a surgeon doesn't know exactly where your heart is and what it's for, but they are going to operate on you anyway," the SANS CTO grins.

Refreshing your knowledge

Reason enough for SANS to develop a training that builds the foundation for a solid career in cybersecurity: SANS SEC275: Foundations. Not only newbie's can benefit from this training, but also students with a background in IT can refresh and grow their knowledge and hands-on skills with it. The people new to the industry were the initial target group for SANS, but to Lyne's big surprise, IT professionals are also enthusiastic about the Foundations training. "Students who don't know much about IT gain a lot of crucial knowledge in a relatively short time, but we also see that people

"THE YOUNGER GENERATIONS ARE A BIT SPOILED WHEN IT COMES TO TECHNOLOGY, BECAUSE 99% OF THE TIME IT JUST WORKS. THAT IS BOTH A GIFT AND A THREAT, BECAUSE IT MEANS THEY NO LONGER LEARN TO FIGURE THINGS OUT FOR THEMSELVES."



who already have this knowledge pick up new things more quickly.” After all, technology is developing at a furious pace and keeping up with it all is virtually impossible. “We see people who once studied computer science, but who have never worked with containers, for example. And virtualisation technology has also changed in recent years. With this training you can brush up your knowledge in these kinds of areas and even learn some new things.”

The ultimate way to learn

SANS Foundations is a very rich e-learning platform with many hours of content in the form of video, audio, study books and over 50 hands-on labs. Especially those labs make the platform engaging and fun for students. “You don’t just learn the theory, you can put it into practice right away”, says Lyne. He challenges students to get off the beaten track and not just follow the instructions of the teachers in the videos. “Trying things out, finding out what doesn’t work, then getting stuck somewhere and figuring out how to make it all work

again in frustration is the ultimate way to learn,” laughs the CTO. “The younger generations are a bit spoiled when it comes to technology, because 99 percent of the time it just works. That is both a gift and a threat, because it means they no longer learn to figure things out for themselves. Whereas the older generation used to have to tinker with things themselves in order to get a video game to work, for example, and therefore quickly learned the basic skills which the younger generation lacks. But you can do yourself a big favour by seeking out that frustration in our hands-on labs, because that struggle really teaches you the basics of IT.”

Closing the skills gap

Lyne’s ultimate goal with SANS Foundations is to close the global cybersecurity skills gap. “We don’t want surgeons without anatomical knowledge. Especially in a world that is changing at lightning speed, where IoT and smart cities will play a big role and AI-systems are ever more evolving, it is important to have a solid foundation of the knowledge

pyramid. I want to help people with a passion for technology get into a cool job market where specialists are in huge demand.” In order to be successful in cybersecurity, the general basic skills are indispensable, the CTO states. “The training from SANS provides exactly what you need to take further steps in cybersecurity,” says Lyne. “IT is such a broad area, but it is not necessary to go into depth on all parts. Then it can get a bit overwhelming. SANS Foundations gives you exactly what its name implies: a solid foundation for additional training in the field of cybersecurity.” For him, it is important that not only IT and cybersecurity specialists gain knowledge and skills, but that other professional groups also become increasingly aware of cyber threats and the ways to work and live safely. “In this way, we are building a pyramid of knowledge and skills that can ensure the digital resilience of the world.”

Distinctive training

The fundamentals training of SANS distinguishes itself from other basic training courses in three ways, Lyne says.

SANS Foundations

Do you want to kickstart a career in IT Security?

"First, the lectures and format are really engaging and fun for students. Those are their words," he hurries to add with a smile. "I think it's really the live demos and hands-on labs that make this course most engaging. You don't just read a book to understand the theory, you actually go and do it. It's much more fun to build a Python program yourself than just reading theory about it." The second thing that really set SANS Foundations apart is the syllabus, which is really tailored to help people study cybersecurity. "As I said, the IT field is huge, but this course is curated to help you succeed in cybersecurity. It is thorough and sufficient, targeted and tailored." Last but not least, the course is constantly updated based on student feedback. "At SANS, we constantly measure student feedback

on content, topics and our labs. We also look at how the market is evolving and try to take all those things into account in continuously improving the course, which really makes a difference."

New features coming soon

"Over the next few weeks, new features will also be added to the platform," says Lyne proudly. "We have some really ambitious plans. There are updates coming for the videos and labs, but we also have a huge set of new features dropping over the next couple of weeks that are the result of feedback from former students that have just started working in cybersecurity. We will add more content about data fundamentals and machine learning. But we have also enhanced our lab systems so they are

even more rich for users to spend time practicing. And for the employers, we will have a refined set of reporting capabilities where they can take a set of students and monitor and encourage their progress throughout the course."

Taking luck out of the equation

Lyne gets really excited talking about this course: "I really wish there would have been something like this when I was setting my first steps in cybersecurity", he grins. "It would have saved me a whole lot of time and frustration!" But what's more, his path into cybersecurity was mostly dictated by luck, "and then hard work and the right mentors". Lyne wants to take the luck part out of the equation for people with the right aptitude, talent and interest in cybersecurity. "I want a more defined path for them. That is what we are trying to reach with SANS Foundations. You shouldn't be dependent on luck to work in the coolest and most interesting industry there is. You should just be able to go for it." 🙌

"YOU SHOULDN'T BE DEPENDENT ON LUCK TO WORK IN THE COOLEST AND MOST INTERESTING INDUSTRY THERE IS. YOU SHOULD JUST BE ABLE TO GO FOR IT."

To learn more about SANS Foundations visit:
sans.org/close-skills-gap

Fortinet Security Fabric

Broad

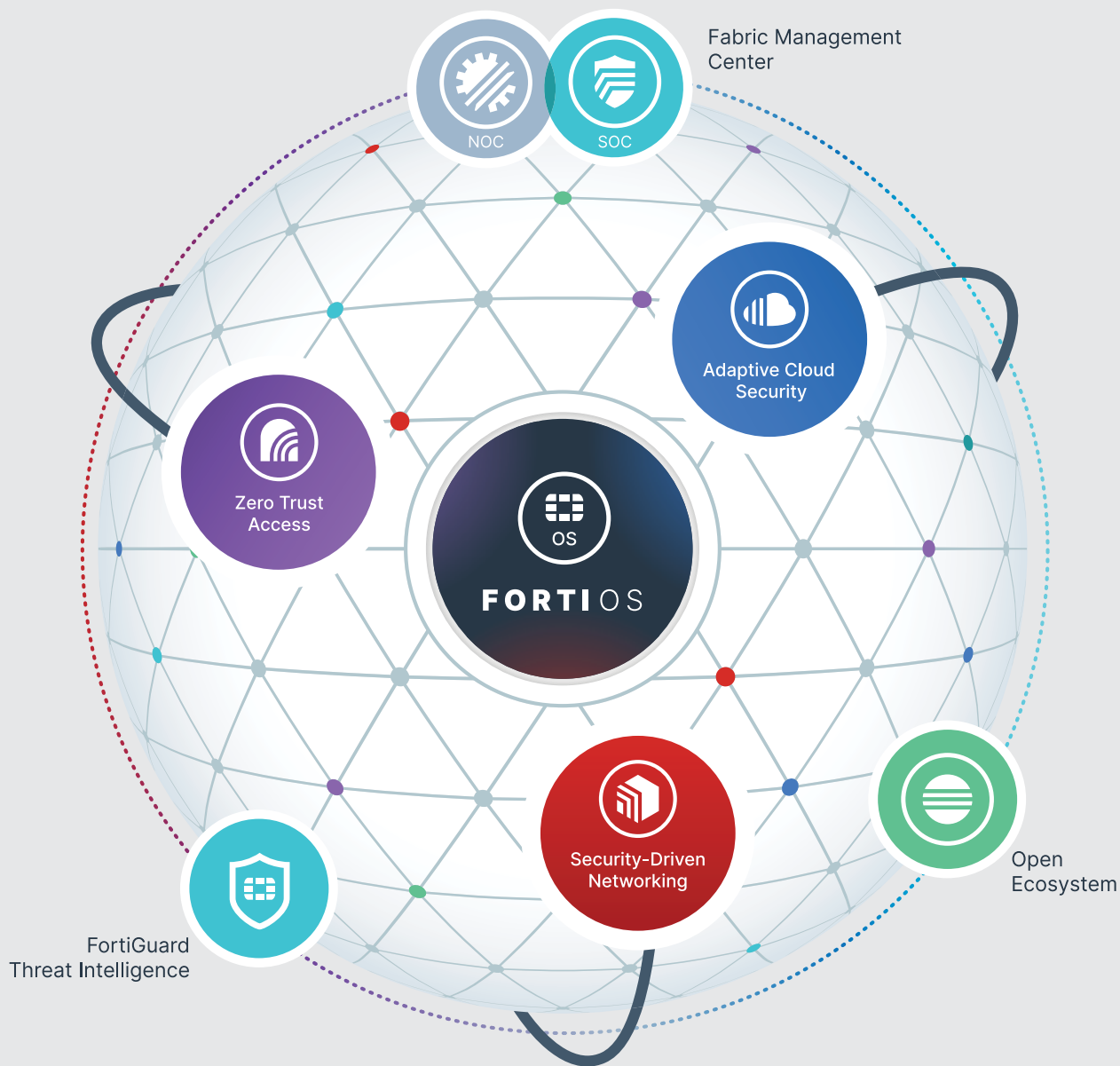
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

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



A STEP AHEAD

WERNO GEVERS, REGIONAL MANAGER AT MIMICAST MIDDLE EAST, ON THE STRIDES AI IS MAKING IN CYBERSECURITY AND HOW THE COMPANY IS LEVERAGING THIS TECHNOLOGY TO PROVIDE INTELLIGENT CYBERSECURITY SOLUTIONS.

What is the exact role of AI in cybersecurity? How do you think it can enhance the threat defences of an organisation?

Attackers constantly evolve their tactics to side-step traditional defences, making it nearly impossible for IT security teams to fight off cyberattacks without the aid of artificial intelligence. By constantly 'learning' an organisation's environment and user behaviours to get smarter over time, AI tools create a baseline of normal, creating detections and alerts for anomalous behaviour.

Machine learning algorithms can help AI become more resilient. Using tactics such as training AI on unique data, analysing patterns of errors in training data, and thinking like an adversary, organisations can use machine learning

to make their AI models more resilient to attacks. Adding a new layer of defence – blocking hard-to-detect threats while alerting and detecting anomalous behaviour – is critical.

How does Mimecast use AI to enhance its security offerings? Also, something about the Mimecast CyberGraph?

Mimecast CyberGraph is a new add-on for Mimecast Secure Email Gateway (SEG) that is engineered to use Artificial Intelligence (AI) to help detect sophisticated phishing and impersonation attacks. CyberGraph creates an identity graph which is built to store information about relationships between all senders and recipients. The graph is designed to detect anomalies and leverages machine learning technology to help organisations stay one step ahead of threat actors by alerting employees to potential cyber threats.

Security controls need to evolve to help evade cybercriminals' relentless and crafty approach. CyberGraph includes three key capabilities engineered to help prevent cyber threats:

Renders embedded trackers useless – During the reconnaissance phase of an attack, threat actors embed trackers into emails that communicate with an illegitimate remote server, disclosing important information that can be used to create a targeted social engineering attack. CyberGraph is built to block this communication, mask the email recipient's location, and prevents attempts to understand engagement levels with the email content.

Uses machine learning to protect from targeted email threats – CyberGraph is designed to create an identity graph by learning about relationships and connections between all senders and recipients. This intelligence is combined with the outputs from machine learning models to detect anomalies that could be indicative of a malicious email.

Engages users with contextual, dynamic warning banners – CyberGraph is engineered to engage users at the point of risk with color-coded banners that indicate the potential nature of a threat. Users are empowered by seeing

“MIMICAST CYBERGRAPH IS A NEW ADD-ON FOR MIMICAST SECURE EMAIL GATEWAY (SEG) THAT IS ENGINEERED TO USE ARTIFICIAL INTELLIGENCE (AI) TO HELP DETECT SOPHISTICATED PHISHING AND IMPERSONATION ATTACKS.”



Werno Gevers

whether an email is safe or potentially nefarious. CyberGraph is built to “crowd-source” threat intelligence, which helps to reinforce the machine learning model. As the risk associated with any given delivered email changes, banners embedded in any similar emails are updated with the latest information, providing ongoing engagement and protection for users.

In your opinion, what type of organisation is best positioned to leverage AI for security: enterprises, or security vendors, and why?

Both, but it’s not always easy for organisations to leverage it effectively. Most enterprises won’t invest directly in AI, as it requires a team of experts, a large budget and lots of data to make it work. For a single enterprise this

doesn’t always make a lot of sense. Most enterprises lack the data and resources to make AI work effectively, and should be focusing on perfecting and operationalising security basics.

Cloud security vendors on the other hand, have access to the relevant data and the right skills, and they also have the scale, scope, and financial resources to put AI techniques to work. Their customer bases should be able to capitalise on this. When implementing security services, organisations should look at how prospective vendors are applying AI to their solutions to provide a better and more efficient service.

What do you think is the biggest challenge organisations face when it comes to implementing AI in cybersecurity?

It’s important to remember that AI is not a silver bullet to the cybersecurity problem. After all, it’s not only organisations and security providers that will be using AI now and in the future. Cybercriminals understand the benefits of AI and how to counteract it’s use in organisations. It’s therefore vital that security teams don’t rely exclusively on AI, as the only measure for cyber defence. Organisations need to adopt a multi-pronged security strategy, that still relies on the human element.

As more cyber resilience strategies begin to adopt AI, it will be vital that people and technology continue to inform one another to provide agile protection against ever-evolving threat landscapes. Innovations such as CyberGraph provide evidence that AI has a promising value proposition in cybersecurity. 🙌

STREAMLINING CYBERSECURITY

IBRAHIM AZAB, REGIONAL SALES DIRECTOR, MEA, CYBER RES, TELLS SECURITY ADVISOR HOW THE CYBERSECURITY LANDSCAPE IS CHANGING AND WHAT ORGANISATIONS MUST DO TO STREAMLINE THEIR CYBERSECURITY APPROACH.



Ibrahim Azab

The cybersecurity industry is in an exciting space today: The constant growth of the attack surface, new attack vectors and the consequent challenge in cyber

defence and methods of resilience, all make it an interesting and creative place to be in.

There used to be a time when organisations had pre-defined assets and perimeters and one policy that ruled them all. Today, technology is the accelerator of development and the security landscape is in a constant flux with cloud services, automation, IoT, hybrid working methods and different data management solutions.

In this context, risk assessment and management, too, have undergone systematic change. Today, it is a constant challenge to find ways to rejig organisational processes, products and procedures to minimise the impact of cyberattacks on people and businesses.

Who's the biggest adversary?

Very often, organisations make the mistake of zeroing-in on the wrong adversary or attack surface as the biggest threat: In my opinion, the single most formidable opponent that all businesses everywhere must fear, is the state of being unprepared. Look at it this way: threats will always happen-in fact, the nature of these will be complex, complicated and unexpected. One only has to look around at the recent cases of devastating cyberattacks

and corporate espionage, to realise this. If organisations do not recognise the signs and begin working on a comprehensive resilience strategy, then that's where the whole problem lies, and such organisations will be the biggest hit. Remember this: there's no such thing as "if" in cybersecurity. With the frequency with which attacks are happening today, the only question is "when."

The numbers challenge

Perhaps, the biggest challenge faced by smaller organisations and businesses today is that of small teams and the fear of signing on large cybersecurity agencies or even appointing a Chief Information Security Officer (CISO). In fact, many of them are content with over-the-counter software to take care of the defence part, which we all know, is hardly enough.

In such cases, I'd recommend two approaches to the problem: If an organisation thinks that it has invested significantly in skills and cybersecurity solutions, then they should consider moving to the next stage: investing in automation solutions. These solutions will take on the level-1 events—those that are most common, giving organisations enough time and space to focus on the more critical, serious attacks.

The second approach for those organisations that lack the necessary cyber defence skills but are growing in every other respect, is to join hands with a cybersecurity agency that will help them build a solid and stable cyber defence mechanism. However, they should be careful selecting the right company, since no two security agencies have the same approach or the same kind of product. Each organisation must sit with the cybersecurity agency, get to know each other well and then come up with a defence strategy that works best.

In each of these cases, though, it is critical to appoint a CISO to take charge of the entire cybersecurity management of the organisation and is engaged full-time in defending important data. Not only must the CISO oversee the security technologies and solutions and define suitable controls and standards based on the company's geographical location

and the regulatory frameworks in place in that location, but he must also implement the entire cybersecurity strategy of the organisation, whether it is done by internal teams or by an outside organisation.

My data is breached, what do I do now?

This is the most important question that businesses ask today. I firmly believe that in this case, the most important thing to do is to communicate and be transparent. Instead of shifting the blame or hiding facts, any organisation that realises it is breached must make sure that all of its employees and stakeholders are made aware of the situation. This is the time to put in place a well-defined communication plan. This allows everyone in the organisation to step up, be alert and involve their teams in planning for co-ordinated activities.

“THE SINGLE MOST FORMIDABLE OPPONENT THAT ALL BUSINESSES EVERYWHERE MUST FEAR, IS THE STATE OF BEING UNPREPARED.”

Secondly, learn from your mistakes. Re-evaluate the cybersecurity strategy and program. Conduct a comprehensive risk assessment to assess the new risk appetite and the defence strategies in place. Optimise the existing technology, people and processes to identify gaps and address issues.

How to streamline the cybersecurity approach

There are five things all organisations must keep in mind to make sure that their cybersecurity strategies work and are resilient enough.

Implement a comprehensive cyber resilience program: For this to happen, companies must have a proper governance

plan that defines ownership, accountability, risks and compliance. Very often, organisations mistake cyber resilience programs for a set of IT procedures or a security policy document.

ta assets: In order to derive maximum value from their data, it is imperative for organisations to understand their data and have an end-to-end privacy policy in place. This framework should comprise deliverables to ensure data resilience, data insights and data usability, throughout the entire data lifecycle.

Understand that cybersecurity is a system, not just technology: It is important to understand that people are as important in a cyber resilience strategy, as technology. So implement technology controls where applicable, but make sure to involve people in the whole program, especially when it comes to reporting security violations or change in governance policies.

Keep policies simple and easy to fathom: This is one of the most important aspects, and yet, the most abused. In order to have a cyber resilience strategy that works, organisations must understand the difference between 'policy,' 'standard,' 'procedure' and 'product.' A policy is a directive that has a goal, enough information to support it and does not change very often. Standard refers to the rubric by which implementation and compliance are measured. Procedures are the immediate steps to achieve the goal, and this can change frequently, from time to time.

Have a crisis communication plan in place: Every organisation **MUST** have a plan to deal with sudden, unexpected disruptions to their business, especially those that threaten its survival. This communication plan should comprise details like how a crisis is tackled, who in the organisation should be the first to deal with it, by when the crisis is expected to be resolved, and specific communication directives to employees and external stakeholders. Each employee and stakeholder must be given clear instructions on their duties at the time, and who is in charge of what—whether it is system restoration or carry out a manual backup or even issue a press/media statement. 🗣️



Mathivanan Venkatachalam

A HOLISTIC APPROACH TO CYBERSECURITY

MATHIVANAN VENKATACHALAM, VICE-PRESIDENT AT MANAGEENGINE, ON THE NEED TO VIEW CYBERSECURITY AS A COLLECTIVE RESPONSIBILITY AND AS A LONG-TERM VISION.



How have the security priorities of organisations changed post the pandemic?

The pandemic changed the way we work, distributing a highly centralised workforce and later pushing organisations into a hybrid work model. The number of devices utilised for remote work increased rapidly, and most organisations were not prepared to support the surge. This increased the attack surface exponentially. Adding to the evolving threat landscape, ransomware attacks have increased by nearly 500% since the pandemic began. To address the escalation of attack surfaces, organisations now adopt a holistic approach and deploy prevention resources like employee monitoring tools, Zero Trust tools, endpoint protection platforms, and endpoint detection and response tools.

With the threat & security landscape rapidly changing and evolving, is the role of the CISO/CIO/IT decision maker changing? What are the new challenges?

Yes, more and more organisations are viewing cybersecurity as the collaborative responsibility of CISOs, CIOs, and business leaders rather than an individual show waged by CISOs alone.

Challenges:

a. In ManageEngine's recent 2021 Digital Readiness Survey, 83% of respondents revealed that having more remote workers

led to an increase in security risks. With a change in the way we work, CISOs need to analyse their existing and new third-party tools for any vulnerabilities that can be exploited by devices on the edge. Third-party cyber hygiene has become increasingly challenging with the expanded reliance on third-party tools.

b. There's been a surge in shadow IT because many employees continue to use third-party applications they grew comfortable working with remotely, bringing these unauthorised tools back into the office network. According to the ManageEngine report, 78% of organisations revealed that remote workers download software without obtaining approval from the IT department.

c. IT teams are facing tighter budgets that focus mainly on business continuity and productivity rather than cybersecurity.

d. Organisations may find it difficult to keep employees cyber-aware as the threat landscape is constantly evolving and make sure they follow cybersecurity best practices.

How can CIOs/CISOs balance the cybersecurity goals of an organisation with the business/financial side?

Although accepted as an indispensable part of most organisations, cybersecurity is still often feared to be an investment that hinders business productivity and exhausts the IT budget.

Based on the vertical they belong to, each organisation has a unique set of security needs. CISOs will have to work together with CIOs and business leaders to figure out their immediate requirements and strike a balance between the organisation's security and business needs.

Business leaders must view cybersecurity as a long-term vision instead and work on executing strategies incrementally. This way, organisations can build a strong cyber defence that can effectively combat the evolving threat landscape. 📌

➔ **“BUSINESS LEADERS MUST VIEW CYBERSECURITY AS A LONG-TERM VISION INSTEAD AND WORK ON EXECUTING STRATEGIES INCREMENTALLY. THIS WAY, ORGANISATIONS CAN BUILD A STRONG CYBER DEFENCE THAT CAN EFFECTIVELY COMBAT THE EVOLVING THREAT LANDSCAPE.”**

STARLINK
TRUSTED CYBER & CLOUD ADVISOR

TRUE VALUE-ADDED
DISTRIBUTOR



STARLINK
TRANSFORMS
WITH INTELLIGENT AUTOMATION

Security

ADVISOR

MIDDLE EAST



SPECIAL REPORT

**PROTIVITI:
LEADING THE WAY**

PROTIVITI-LEADING THE TECHNOLOGY CONSULTING PRACTICE IN THE MIDDLE EAST

WITH THE GLOBAL BUSINESS LANDSCAPE BECOMING INCREASINGLY VOLATILE AND DIGITAL TRANSFORMATION ON THE ASCENT, THE NEED FOR EXPERT INSIGHT AND FUTURISTIC VISION BECOMES IMPERATIVE. ANITA JOSEPH, EDITOR, SECURITY MIDDLE EAST, CAUGHT UP WITH SENIOR EXECUTIVES AT PROTIVITI MEMBER FIRM FOR THE MIDDLE EAST REGION, A GLOBAL BUSINESS CONSULTING FIRM, TO UNDERSTAND HOW THEY HELP BUSINESSES ADDRESS CHALLENGES AND OPPORTUNITIES IN KEY AREAS SUCH AS TECHNOLOGY, DIGITAL TRANSFORMATION, BUSINESS PROCESS IMPROVEMENT, RISK MANAGEMENT, COMPLIANCE, TRANSACTION ADVISORY AND INTERNAL AUDIT.



“PROTIVITI IS BUILT ON VALUES OF INCLUSION AND DIVERSITY, AND WE ARE HIGHLY MOTIVATED BY THIS PURPOSE. THIS MEANS THAT PROTIVITI NOT ONLY LEVERAGES THE LOCAL TALENT IN THIS REGION BUT ALSO HARNESSES THE POTENTIAL OF THE YOUTH AND CONTRIBUTES TO THEIR GROWTH.”

Arindam De, deputy CEO, Protiviti Member Firm for the Middle East Region.

As digital transformation gathers steam, and the business landscape becomes increasingly complex - full of rapidly shifting consumer preferences and new operating models, the need for the right advice and timely insights are becoming more important than ever. Unfortunately, the plethora of solutions and technologies available today have made it difficult to see in the fog, and the relevant expertise remain elusive. This is where Protiviti steps in, with its extensive insights, tailored approach, and unparalleled collaboration ecosystem. In fact, it's innovation-centric processes, futuristic vision and values of inclusion have made it a force to reckon within the Middle East region. The firm has been part of many strategic consulting engagements in the region over the last decade-and-a-half, successfully delivering on engagements across diverse industries, and supporting businesses achieve their technology adoption and digital transformation



Ranjan Sinha



Adib Ibrahim



Mohammed Arshad Hussain



Niraj Mathur



Ramakrishnan Viswanathan



Rohan Lasrado

objectives. Globally, Protiviti was named to the 2021 Fortune 100 Best Companies to Work For® list and has served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

"Protiviti is built on values of inclusion and diversity, and we are highly motivated by this purpose," says Arindam De, deputy CEO, Protiviti Member Firm for the Middle East Region. "This means that Protiviti not only leverages the local talent in this region but also harnesses the potential of the youth and contributes to their growth. Due to the high standards of education in the region, we're seeing more and more technology-oriented resources adding enormous value to organisations and to their entire digital transformation journey," he adds.

The firm has been involved in several key projects in the region where it is working closely with stakeholders to enable digital services for local communities. "One recent example is where we have delivered on a new digital platform allowing subscribers to view and manage their shipments and digital communication online for federal government organisations," says Ranjan Sinha, managing director, leading the technology consulting practice in the region. "We're also working in the areas of stitching and operating fintech platforms and recently we became operators for a supply chain financing platform that facilitates seamless transition and adoption for organisations in the region to minimise discrepancies in financial instruments and provide assurance on delivery and project completions."

That's not all: Protiviti is also working on projects, helping government organisations with issues such as data privacy and security to make sure that the journey towards digital,

and in some cases cloud, is well managed. "We are collaborating with many of our long-time global partners and alliances in product space to offer these services to our clients in the region. We are also working on other initiatives around digital learning experience projects with various government organisations," Ranjan adds.

For Protiviti, its partner ecosystem is equally vital to the long-term success and futuristic strategies of the firm. As Adib Ibrahim, managing director – Technology Strategy & Operations points out, "Alliances and partnerships help us offer full set of solutions to our clients across technology and digital domains. We work with alliance partners to jointly develop go-to-market strategies for clients who are looking for both consulting and implementation services." Elaborating further on the partnership ecosystem Rohan Lasrado, Managing Director, Alliances adds:

"We have built alliances across technology domains, ranging from digital experience and automation, integrations, business apps including ERPs and CRMs, technology operations, security, privacy and cloud by embedding technology automation."

The firm has devised an "agile" approach to building up infrastructure and resource capabilities to address client demands in a rapidly changing technology landscape. Since the pandemic, cloud adoption in the region has been growing at a fast pace. To cater to this niche requirement of organisations and to support their transformation initiatives, Protiviti offers a wide gamut of services, intended to assist organisations to decipher the complexity of cloud.

"We have taken an agile and hybrid approach for addressing this market need, whilst constantly assessing and evolving our service delivery models to meet client expectations," points out Mohammed Arshad, managing director for Emerging Technology Solutions, "Whilst we are building capacities of our own with the right infrastructure and resource capabilities to scale up, we are also working with our key alliances and partners to source required capabilities on need basis, including cloud solutions. Further, we are also addressing the expectations of each country in our region of operations to build infrastructure and resource capabilities, catering to the demand, in alignment with local regulatory requirements."

What's interesting here is the approach that Protiviti has developed towards combining technology adoption with its expertise in risk & compliance, as one of the leaders in Financial Service space. For this purpose, the firm has joined hands with several FinTech, RegTech and SupTech solutioning players to deliver end-to-end value proposition for clients, in the areas of functional advisory, data management and solution implementation. Ramakrishnan Viswanathan, managing director - FS Technology cites a case in point. "Our collaboration with Monimove, which is a leading supply chain finance solution provider allowing organisations to bring their

"ALLIANCES AND PARTNERSHIPS HELP US OFFER FULL SET OF SOLUTIONS TO OUR CLIENTS ACROSS TECHNOLOGY AND DIGITAL DOMAINS. WE WORK WITH ALLIANCE PARTNERS TO JOINTLY DEVELOP GO-TO-MARKET STRATEGIES FOR CLIENTS WHO ARE LOOKING FOR BOTH CONSULTING AND IMPLEMENTATION SERVICES."

entire supply chain value stream on a single platform. This not only enables the supply chain finance ecosystem, but also provides the firms with complete visibility across the supply value chain that will enhance overall governance and help them mitigate operational risk."

As central banks in the GCC region are digitising their supervision function, Protiviti teams are working with regulators to streamline data management and implement RegTech, SupTech solutions, and are looking to collaborate with providers like FNA."

That's not to say data security and privacy isn't at the top of the firm's agenda. As Niraj Mathur, managing director for Security and Privacy Solutions mentions, "We see a major change in the approach towards security in the past decade, privacy on the other hand has become a major concern for organisations over the past 5 years. The security and privacy concerns are consistently amongst the top concerns of not only CISOs or CIOs but for CEOs and the board members as well. The same has been highlighted in our latest edition of Top Risks Report 2021."



Protiviti's research findings indicate that security is at the top of every organisation's business agenda today, because of the following factors:

1. Huge increase in cybercrime incidents
2. Impact of incidents is tangible and directly to the business i.e. loss of revenue, reputational loss which leads to the need for accountability.
3. Increasing awareness amongst senior management
4. Regulatory Frameworks and cyber security / privacy laws
5. New risks emerge as organisations adopt digitisation, a necessity for most businesses.

"We are in a dynamic environment today



We have taken an agile and hybrid approach for addressing this market need, whilst constantly assessing and evolving our service delivery models to meet client expectations.

where security and privacy cannot be ignored or become an afterthought. A lackluster approach towards security can negatively impact the P&L statements today and organisations could lose their hard-earned profits, due to incidents or pay hefty fines. Organisations have realised cybersecurity risks are not an IT issue, it's a board level concern. At the same time, the attention paid to security and privacy is only expected to increase with more maturity setting in [GCC regulatory laws and focus on compliance] as we move forward," Niraj adds.

The firm has strongly leveraged its rich experience, stemming from executing complex engagements across diverse client base and industries in the region. It also has market

access and coverage to continuously build and enhance large scale delivery centers, capable of delivering onshore/ offshore services or through hybrid models across GCC, India and Egypt.

While the tech consulting team at Protiviti seems geared up for a strong growth trajectory as it bridges the gap between business needs of its clients and strong portfolio of technology solutions, there is the challenge of talent shortage and domain skill that could be a matter of concern.

According to Arindam, talent is at times inherent with existing resources, and many a times, is required to be built upon within the organisation through learning and development initiatives. "Although it can be a long journey, it

provides assurance that the talented resources of our organisation get the opportunity to pursue fields that they are most inclined towards. Certainly, there are challenges in hiring talent for niche and growing areas of technology such as cloud computing, cyber security etc. However, we tackle it by sourcing the requisite talent from anywhere in the region, at the same time also nurturing our existing resources into these niche areas. Protiviti's consulting portfolio is now ahead of the curve in assisting industries for technology adoption. We consistently assess market needs and also rely on internal and external market intelligence to forecast and meet the diverse needs of the GCC market," he concludes. 🙌

QUALYS OFFERS FREE RANSOMWARE RISK ASSESSMENT & REMEDIATION SERVICE

Qualys, Inc, a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions, has announced the availability of its Ransomware Risk Assessment Service to provide companies with visibility into their ransomware exposure and automate the patching and configuration changes needed to reduce risk immediately. As part of Cybersecurity Awareness Month and to help organisations proactively combat ransomware, Qualys is making the solution available at no cost for 60 days.

Ransomware continues to escalate with the FBI reporting a 62% year-over-year increase for the period ending July 31, and President Biden convening with global leaders in an effort to protect economic and national security. Unpatched vulnerabilities, device misconfigurations, internet-facing assets and unauthorised software rank

consistently among the top attack vectors. Authorities like CISA and NIST recommend that organisations strengthen their defense by proactively assessing ransomware risk including quickly patching associated vulnerabilities.

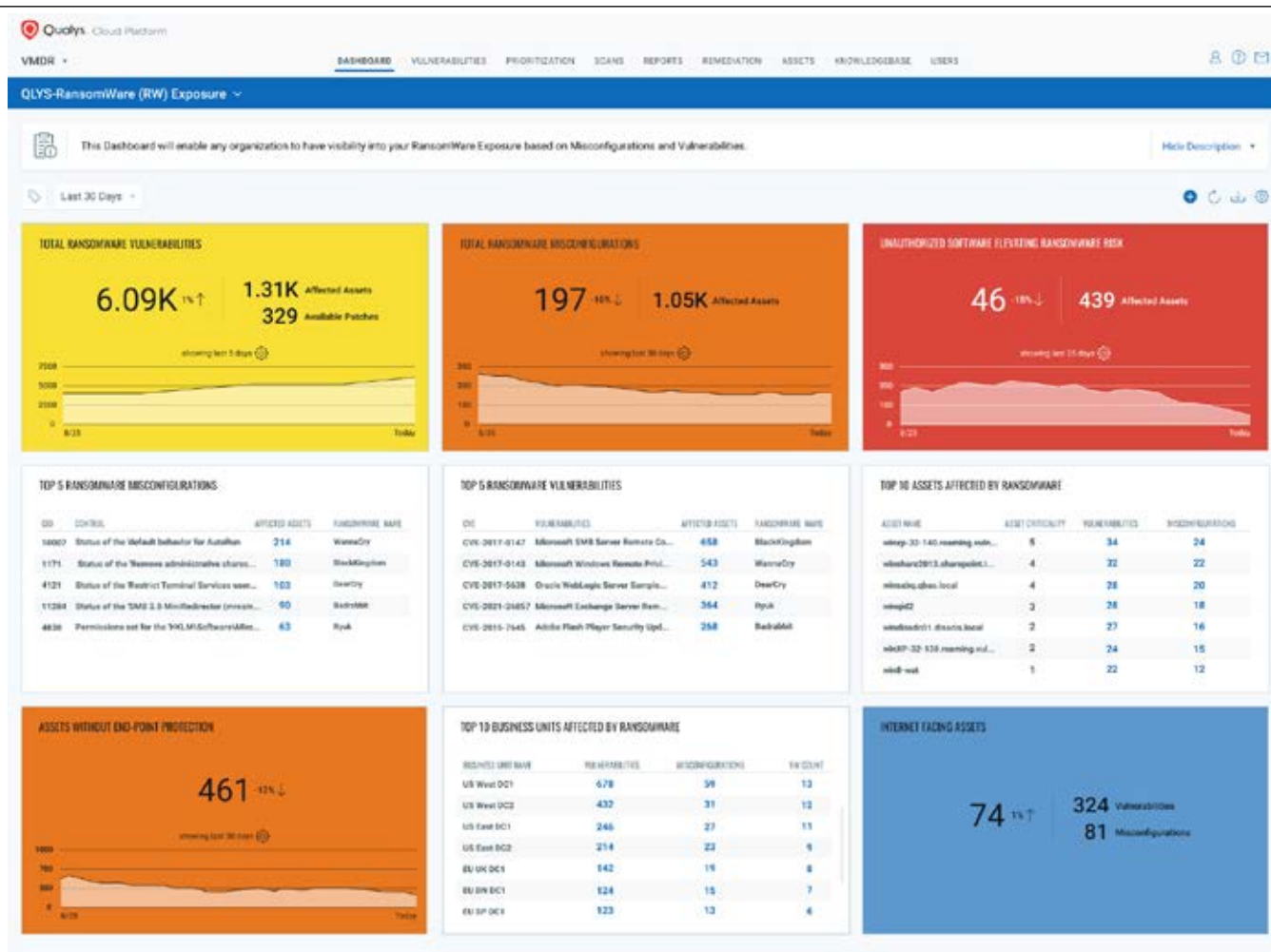
“While there is no silver bullet to prevent ransomware, companies can take charge with proactive measures including solid cybersecurity hygiene, patching for known ransomware vulnerabilities, changing configurations and adjusting security policies,” said Jim Reavis, co-founder and CEO of the Cloud Security Alliance. “Qualys Ransomware Risk Assessment puts cybersecurity teams in control by operationalising government guidelines and providing a company-specific ransomware heatmap so they can eliminate an area of risk and shrink their attack surface.”

Qualys vulnerability and threat researchers analysed ransomware

attacks over the last five years to identify approximately 100 CVEs commonly used by ransomware threat actors. Researchers mapped CVEs to ransomware families like Locky, Ryuk/Conti and WannaCry along with specific misconfigurations that are typically leveraged by the threat actors.

Leveraging the research, Qualys developed the Ransomware Risk Assessment Service, powered by the VMDR platform, to help organisations proactively identify, prioritise, track and remediate assets that are vulnerable to ransomware attacks. Once identified, vulnerabilities are mapped to available patches that can be directly deployed from the service without requiring additional tools and VPNs reducing the company’s ransomware exposure.

Qualys Ransomware Risk Assessment Service leverages a single, dynamic dashboard to provide a clear



comprehensive view of your ransomware risk exposure including:

Identification of Internet-facing assets

The solution includes comprehensive asset discovery and a global asset software inventory that identifies and highlights internet-facing assets and unauthorised software to eliminate security blind spots.

Clear insights into ransomware exposure

Expertly researched and curated ransomware-specific vulnerabilities and misconfigurations provide actionable insights so security teams can prioritise workflows and take immediate steps to reduce ransomware risk. Teams can also track remediation progress via live dashboards that provide clear metrics.

Integrated patch deployment

One-click and zero-touch workflows kickoff

“WHILE THERE IS NO SILVER BULLET TO PREVENT RANSOMWARE, COMPANIES CAN TAKE CHARGE WITH PROACTIVE MEASURES INCLUDING SOLID CYBERSECURITY HYGIENE, PATCHING FOR KNOWN RANSOMWARE VULNERABILITIES, CHANGING CONFIGURATIONS AND ADJUSTING SECURITY POLICIES.”

remote vulnerability patching regardless of the asset location. Since the solution is cloud-based, the need for on-premises patching tools that require VPNs is eliminated.

“Ransomware risk is top of mind for CISOs who are no longer satisfied with reactive tools and generic guidelines. They want actionable information to reduce risk proactively,” said Sumedh Thakar, president and CEO of Qualys. “The Qualys security team has extensively researched past ransomware attacks as well as CISA, MS-ISAC and NIST guidance and operationalised it into a prescriptive, actionable plan so companies can proactively remediate to stay ahead of ransomware attacks and reduce their overall risk.”

Availability

The Qualys Ransomware Risk Assessment Service is available immediately. 📌

NETWITNESS ANNOUNCES KEY SALES APPOINTMENT IN EMEA REGION

■ SECURITY INDUSTRY VETERAN MASSIMO VULPIANI IS PROMOTED TO LEAD EMEA SALES.



Massimo Vulpiani

VULPIANI HAS BEEN A KEY CONTRIBUTOR WITH RSA FOR OVER 20 YEARS. HE MOST RECENTLY HELD COUNTRY AND REGIONAL DIRECTOR LEADERSHIP POSITIONS AND GREW REVENUE BY MORE THAN 25% WHILE LEADING THE SOUTHERN REGION OF EMEA.

NetWitness, an RSA business (@RSAsecurity), a globally trusted partner for some of the world's largest and most security sensitive organisations, has announced a key promotion within its sales organisation in the EMEA region. Long-time security industry veteran Massimo Vulpiani has been promoted to lead NetWitness sales across Europe, the Middle East and Africa.

"I'm excited to announce Massimo's promotion and expanded role," said Dave Govan, chief revenue officer at NetWitness. "Massimo has vast experience in our space

and fully understands the needs of our large enterprise customers and our strategic channel partners as we continue to provide our technology and services for their most critical cyber security in the areas of incident response, threat detection and response for cloud, network, SIEM, endpoint and IoT. Threats are continually evolving as are our offerings. Massimo will be instrumental as we continue to work together with our customers and partners," Govan added.

Vulpiani has been a key contributor with RSA for over 20 years. He most recently held country and regional director leadership positions and grew revenue by more than 25% while leading

the southern region of EMEA. Following the re-configuration of RSA's business units, Vulpiani led NetWitness sales leadership for South Europe. Prior to his time at RSA, he held roles at the Joint Research Center in the European Commission, Computer Associates and Symantec. Vulpiani has studied at the International Institute of Management Development, the SDA Bocconi School of Management and the University of Milan.

"I'm energised to take on this new challenge and help enterprises in EMEA build upon their cybersecurity strategies with NetWitness' threat detection and response capabilities," Vulpiani said. "Threats are growing in number and complexity every day – it's critical that security teams have the visibility and analytics they require to take quick action to mitigate the impact of attacks." 📌

17-21 OCT 2021

DUBAI WORLD TRADE CENTRE



GITEX
TECHNOLOGY
WEEK

X



Fintech
SURGE.
فنتك سبرج

FUTURE
BLOCKCHAIN
SUMMIT
قمة مستقبل البلوك تشين

ماركتنغ مانيا
Marketing
Mania

17-20 OCT 2021

WHERE BUSINESS,
INNOVATION,
AND THE FUTURE
WILL BE DECIDED

140 COUNTRIES PRESENTING THEIR TECHNOLOGIES,
MAKE SURE YOU'RE THERE TOO

SECURE YOUR SPACE NOW: marketing@gitex.com

#GITEX2021
GITEX.COM

Gold Sponsor



5G Innovation Partner

Bronze Sponsor



VIP Majlis Sponsor



Platinum Sponsor



نيوم NEOM

Conference Sponsor



Headline Sponsor
Xlabs



Headline Sponsor
Xlabs



Supporting
Sponsor Xlabs



Supported by



Organised By



SECURING THE CONNECTED LANDSCAPE

SAKKEER HUSSAIN, DIRECTOR - SALES & MARKETING, D-LINK MIDDLE EAST & AFRICA, ON HOW THE DEMAND FOR SECURE AND RELIABLE MANAGED WIFI SOLUTIONS IS NOW STRONGER THAN EVER, WITH ORGANISATIONS FOCUSING ON SECURITY AT THE CORE OF THEIR BUSINESS.



Sakkeer Hussain

With remote working/cloud computing becoming increasingly popular, the security of devices is top priority for both organisations and employees now. How does D-Link ensure the security of its remote and managed Wi-fi devices?

Hybrid or remote work is here to stay. With this in mind, it is now more important than ever for organisations to provide their employees with robust, reliable and secure network connectivity.

D-Link's wireless and cloud-managed devices are designed with security in mind. Our Nuclias Cloud Access Points are equipped with the latest 128-bit Personal and 192-bit enterprise encryption, which protects customers' business and its data from malicious motives. It gives network administrators better control and visibility over their wireless access points, giving them peace of mind as they enable their respective organisations to achieve increased productivity and business resilience.

At D-Link, we are continuously

innovating to make sure that our products and services are designed with security at the core. In addition, we constantly working with our technology and channel partners to ensure that our customers in the region are well-equipped and adept to effectively leverage our solutions to achieve their secure connectivity needs.

What are some of the top security trends in this space (remote/hybrid work) at the moment? What is it that customers insist on the most?

As customers embrace remote and hybrid work models for their businesses, security is increasingly being prioritised. Adversaries exploit the same advanced technologies that businesses use and take advantage of any vulnerabilities. With hybrid work models, there is an immediate need to secure the collaboration tools that are used for business. Companies must also secure their data, assets and applications as they embrace multi-cloud environments. Also, companies have to establish stronger access control solutions since remote workers need to be able to access corporate data from where ever they are. Data security is another important area where organisations have to increase their focus. With long-term hybrid work plans in place, who and how corporate data is used is of utmost significance.

The most important element that customers are emphasising on are having seamless networking

and connectivity solutions. All the technologies that are adopted in hybrid models will not work well without strong, fast and secure Wi-Fi connections.

What are some of the security challenges faced while implementing a smooth and seamless remote working process? How do you address these challenges?

One of the primary challenges is the expanded attack surface. With employees working from home, they are no longer covered by the tools and monitoring on company's corporate network. This means that customers' security teams are under extra pressure to employ safeguards on networks that employees use every day. This requires businesses to rethink their security strategies to account for many more potential vectors for attacks.

Another big challenge is around data security. Data is now no longer confined to the walls of a physical office. With remote working, employees use their own personal devices and often access public Wi-Fi networks.

This needs to be seriously addressed by customers by enhancing user awareness and sharing best practices. Weak passwords that are not regularly updated is yet another issue. Companies need to encourage employees to have strong security hygiene, ensuring that they employ the necessary preventive measures against cyber-attacks

including adopting a secure home Wi-Fi connectivity as well as leveraging strong passwords for their devices.

Also, while implementing hybrid work models, backup and recovery systems are not thought of. If an employee's personal device gets compromised and it happens to be the same device he uses for work, there are high chances that company data will be lost without any backups.

Organisations must also invest in robust data security solutions and purchase products and solutions that have security deeply integrated into them.

Addressing today's security challenges comes down to establishing clear security policies and ensuring employees are aware of the consequences. Now more than ever, it is vital for organisations to understand that security is everyone's responsibility.

What is your forecast for the remote device/managed Wi-fi security market in 2022?

What became pertinent over the last few months is that the future of work is hybrid. With organizations across multiple industries revealing plans to continue operating in hybrid models, insecure devices accessing corporate WiFi will pose a significant threat. We can expect cybercriminals to continue to take advantage of this moving forward. A study by Cybersecurity Ventures forecasts that global cybercrime costs will reach \$10.5 trillion by 2025. This means that organisations need to ensure that they put security at the core of every aspect of their business spanning from endpoints to the network. This will further drive the demand for secure and reliable managed WiFi solutions. With tools such as the Nuclias Connect and Nuclias Cloud, businesses can benefit from not only seamless network access and unlimited scalability but also advanced security. 📌

→ **“ADDRESSING TODAY’S SECURITY CHALLENGES COMES DOWN TO ESTABLISHING CLEAR SECURITY POLICIES AND ENSURING EMPLOYEES ARE AWARE OF THE CONSEQUENCES.”**

SECURITY RISKS IN NEW ERA OF REMOTE WORKING A CAUSE OF CONCERN FOR UAE IT LEADERS: THALES SURVEY



John Doley

C OVID-19 quickly ushered in the era of remote work, introducing new risks that IT professionals are struggling to manage with existing security tools, according to a new Thales study. Six in 10 UAE respondents said traditional security tools such as VPNs are still the primary vehicle for employees accessing applications remotely -- likely the reason why 87% were concerned about the security risks/threats of employees working remotely.

These are among the key insights from the 2021 Thales Access Management Index, a global survey of 2,600 IT decision makers, commissioned by Thales and conducted by 451 Research, part of S&P Global Market Intelligence, to better understand the new security risks and challenges caused by the rise of remote working and cloud transformation caused by the COVID-19 pandemic.

Last year saw a surge in cybercrime exploiting the various aspects of the COVID-19 pandemic and the shift to remote work, with ransomware attacks soaring by 150%. The Thales survey found the pandemic's effects have had a significant impact on security infrastructure,

particularly on access management and authentication frameworks, pushing organisations to adopt modern security strategies like Zero Trust to support the demands of a more mobile and remote workforce.

Era of Remote Working – Concerns Catalyse Change

According to the index, respondents have many different systems deployed for remote access. When asked about the technologies that were in place, VPN was the most common, with 60% of IT professionals identifying the capability. Virtual Desktop Infrastructure, cloud-based access and Zero Trust network access/software defined perimeter (ZTNA/SDP) closely followed. However, when asked what new access technologies respondents were planning to deploy due to the pandemic, nearly half (44%) indicated ZTNA/SDP was the top technology choice.

Thales also explored respondents' plans to move beyond traditional VPN environments, and found that nearly 40% expect to replace their VPN with ZTNA/SDP, while 38% expect to move to a Multi-Factor Authentication (MFA) solution. This confirms the need for more modern, sophisticated authentication capabilities is driving change in many organisations and is perceived as a key enabler of Zero Trust security.

"Seemingly overnight, remote access went from being an exception to the default working model for a large swath of employees. As a result, businesses are navigating a volatile and complex world, and adopting a Zero Trust model of cybersecurity will enable them to continue to conduct operations safely amidst the uncertainty," said John Doley, director for Access Management at Thales for META region. "One of the core barriers businesses face when starting their Zero Trust journey is the balance between locking down access without interrupting workflow. People require access to sensitive

THE THALES SURVEY FOUND THAT THE PANDEMIC'S EFFECTS HAVE HAD A SIGNIFICANT IMPACT ON SECURITY INFRASTRUCTURE, PARTICULARLY ON ACCESS MANAGEMENT AND AUTHENTICATION FRAMEWORKS, PUSHING ORGANISATIONS TO ADOPT MODERN SECURITY STRATEGIES LIKE ZERO TRUST.

data in order to work and collaborate and business leaders will need to ensure that a drop in productivity doesn't become an unwanted side effect. The research shows that IT professionals increasingly see access management and modern authentication capabilities as key components in achieving a Zero Trust model."

Room to Grow with Zero Trust

The Thales report found that Zero Trust models are the solution of choice for respondents seeking to improve access environments, yet many are still in the early stage of adoption.

According to the research, less than a third (30%) of the respondents claim to have a formal strategy and have actively embraced a Zero Trust policy. Additionally, almost half (45%) are either planning, researching or considering a Zero Trust strategy. Surprisingly, less than a third (32%) of the respondents indicated that Zero Trust

shapes their cloud security strategy to a great extent.

Access Security Needs to Adapt to Deal with Dynamic Workplaces

A silver lining of the pandemic-driven rush to remote working is the acceleration of improved approaches to access security. Thales found that 55% of respondents currently have adopted two-factor authentication within their organisations. Regionally, there was notable variation, with the UK leading (64%), followed by the U.S. (62%), APAC (52%) and LATAM (40%). These varying degrees of adoption may be due to the level at which better access management is prioritised in security investments.

Yet, despite the well-known limitations of passwords, investment in MFA still trails other security tools like firewalls, endpoint security, SIEM and email security. Remote access users are still the main use case for MFA adoption (71%). One-third of respondents that have adopted MFA use more than three different authentication tools, signaling the need for a more unified approach to access management in the future.

Another crucial element is the awareness of the workforce about the threat landscape that emerges with remote working practice. Human factor is key pillar in cybersecurity and having people well trained paradigm is essential to minimise the risks of the new risks induced by remote working.

"Security tools and approaches need to adapt to better support the era of remote working," said Eric Hanselman, chief analyst at 451 Research, part of S&P Global Market Intelligence. "The shift towards a Zero Trust model, along with increasing use of modern authentication technologies, like adaptive and multifactor authentication (MFA), will improve organisations' security posture. This will be an exciting space to watch as businesses continue to deal with dynamic workplace environments." 🧑🏻

THE DECISION DILEMMA

ANITA JOSEPH, EDITOR, SECURITY MIDDLE EAST, SITS DOWN WITH CISOS/CIOS AND IT DECISION MAKERS TO FIND OUT HOW THEIR WORLD HAS CHANGED.

The role of the CISO50 is becoming more important today than it has ever been. 2021 being the year of rapid transformation and recovery from the impact of the pandemic, the conversation around security is front and center. So much so that it's become top priority for business leaders as the world prepares to recover from the damages of 2020. This puts the Chief Information Security Officer and other security professionals in the hot seat — from the weekly IT department stand-up to the quarterly board meetings.

What are the challenges that they face as they steer their companies through uncertain times? What is their strategy for success? This is the conversation that no business can afford to miss today.

To begin with, how have the security priorities of organisations changed post the pandemic?

Avinash Advani, founder and CEO at CyberKnight, says there are several key dynamics being considered in upcoming plans that put cybersecurity at the top of the board agenda. "Firstly, security decision makers are now looking to optimise their secure remote access as well as cloud architectures, since many organisations were thrown into work-

from-home mode overnight when the pandemic struck. They instantly realised the inefficiencies and pitfalls of traditional security infrastructures. Secondly, as the perimeter suddenly grew exponentially with remote working, managing trust became a challenge, and ensuring that the right users, applications, and devices were given access to sensitive data became even more critical. Thirdly, digital transformation initiatives have accelerated and complex hybrid environment that ensue, naturally introduce security gaps which need to be bridged with intelligent cybersecurity. Lastly, cyber-attackers have been taking advantage of the expanded attack surface

and the number and types of attacks have increased dramatically.

According to Cherif Sleiman, chief revenue officer, EMEA at Safe Security, no organisation could have planned for Covid-19 or had a business continuity plan that factored in an event like this. "Prior to the pandemic, employees were tethered to the office, using specific devices plugged into a specific corporate network at a specific time of the day to access applications required for them to do the job. From a security standpoint, there were clear organisational borders, centred around the data centre that was akin to protecting a fortress. Post pandemic, the world experienced a seismic change. Remote working and the hybrid workplace have become the norm. With limited/ no access to their data centers during the pandemic, organisations have had to rely on SaaS and Cloud technologies for business continuity. This has spawned the age of the borderless enterprise."

Mohammed Al-Moneer, regional



Avinash Advani
founder and CEO at
CyberKnight

director, Middle East, Turkey & Africa at Infoblox says the pandemic has dramatically refocused business priorities for businesses across the globe. "In a life before Covid, businesses prioritised factors such as increasing operational productivity, communicating better with other departments and gaining better control over day-to-day financial processes. The focus now is on being able to adapt to Digital Transformation in order to remain operational, and in



Cherif Sleiman
chief revenue officer,
EMEA at Safe Security

"IN A LIFE BEFORE COVID, BUSINESSES PRIORITISED FACTORS SUCH AS INCREASING OPERATIONAL PRODUCTIVITY, COMMUNICATING BETTER WITH OTHER DEPARTMENTS AND GAINING BETTER CONTROL OVER DAY-TO-DAY FINANCIAL PROCESSES. THE FOCUS NOW IS ON BEING ABLE TO ADAPT TO DIGITAL TRANSFORMATION IN ORDER TO REMAIN OPERATIONAL, AND IN THIS SCENARIO, SECURITY HAS BECOME A TOP PRIORITY."

this scenario, security has become a top priority," he says.

Harish Chib, vice-president, Middle East & Africa at Sophos says that post the pandemic, some businesses found it difficult to provide connectivity while others were not prepared to shift to remote working seamlessly. "All these reasons, and more, meant that some businesses were taking temporary shortcuts to enable remote working which led to a worsening of their security posture."

Morey Haber, chief security officer



Mohammed Al-Moneer
regional director, Middle East,
Turkey & Africa at Infoblox

breach can still occur.”

Sam Curry, chief security officer at Cybereason is of the opinion that post the pandemic, teams’ focus on work-from-home and work-from-anywhere has become more mature and accepted.

“Also, an awareness of privacy, safety and

security need to evolve to handle new, insecure environments. Perhaps most critical is the use of cloud services for productivity and security, driving new cloud protection and extended detection & response (XDR). Lastly, you can’t talk about lessons learned during COVID without mention of increased awareness of ransomware and supply chain attacks.”

Avinash Advani points out that the roles aren’t changing per se, they are just becoming that much more important, and reporting up to the board regularly is part of the new normal.

“The new challenges that these leaders face include doing more with less, e.g., covering more requirements with less budget, addressing cybersecurity goals with limited resources, consolidation of tools but with more coverage etc,” he adds.

Tamer Nasrawin is of the opinion that growing business challenges are motivating organisations to go above and beyond to grow and retain their customer base. “Competition is growing and customers are no longer loyal to brands. They’re constantly looking for better experiences, leading them to be more agile.

Ultimately, the delivery of a secure customer experience is key.”



Harish Chib
vice-president, Middle East
& Africa at Sophos



Morey Haber
chief security officer
at BeyondTrust

at BeyondTrust, has another view. “The security landscape, over the past few months, has evolved from protecting against a breach to having the proper procedures, policies, and disclosures for when a breach occurs. The community has come to an understanding that even with the best tools and diligence, a

“WHILE THE CISO/ CIO AND THEIR TEAMS WILL CONTINUE TO CHAMPION THE SECURITY OF THE ORGANISATION, THEY NEED TO PARTNER WITH FUNCTIONS LIKE HUMAN RESOURCES, GRC AND OTHERS TO HOLISTICALLY TACKLE THE CHALLENGE.”

Clearly, the security priorities of organisations have changed, and so have the responsibilities of the security decision makers. Cherif Sleiman points out that pre-pandemic, in a static work environment, the CISOs/ CIOs/ IT managers knew what to look for when identifying security vulnerabilities. "The organisation could have very prescriptive and quantifiable procedures and policies as part of the security handbook." But now, things have changed. "While the CISO/ CIO and their teams will continue to champion the security of the organisation, they need to partner with functions like Human Resources, GRC and others to holistically tackle the challenge. With risk being the ownership of C-level management, moving forward, the role of CIO/CISO is to table Cyber Risk as a board level discussion and initiative to create the awareness needed at that level," he adds.

For Harish Chib, a good start for CISO/ CIO/IT decision makers is to build a solid security foundation. "This includes having the right people, processes and tools in place to give you a fighting chance. A robust security culture ensures everyone is 'on duty' when it comes to protecting the enterprise. Clear, easy-to-follow, and conservative processes will prevent simple mistakes from harming your business. Using the very latest prevention and protection technologies will defend your organisation against attackers when the first two fail. Taken together, these three are just a starting point on the never-ending road to a mature security program."

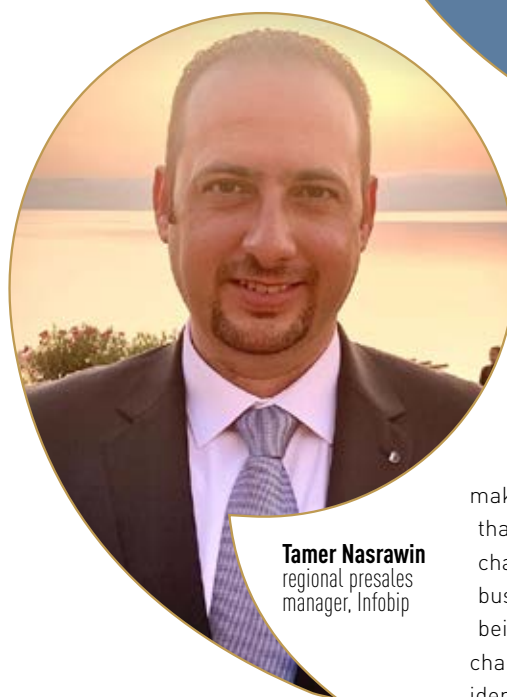
Mohammed Al-Moneer is of the view that the COVID-19 pandemic has highlighted the need for collaborative tools and remote working capabilities for businesses to remain relevant. In this scenario, he says, "the CIO/ CISO has found himself/herself on the front line. The role has become crucial for business continuity and is expected to grow in importance in the coming months.

To cope with these changes and deal with the post-COVID-19 era, he/she must prepare for many challenges ... things like focusing on cybersecurity to resist attacks, setting up a survival plan, setting up a recovery plan and implementing revitalisation actions."

Morey Haber says that today, no one department can mitigate



Sam Curry
chief security officer
at Cybereason



Tamer Nasrawin
regional presales
manager, Infobip

a CFO, legal counsel and even head of go-to-market since the risks for them are all human-derived and adversarial. It is essentially to track operational, legal, IT, finance and security risk independently and as a general risk function," he adds.

Tamer Nasrawin says "IT decision-makers need to implement a strategy that addresses evolving security challenges and fast-changing business challenges. For example, being available across multiple channels is the new norm. However, identifying secure yet flexible solutions and providers to deliver this is will be challenging. Organisations need to assess if this provider is capable of providing agile solutions that are aligned with their business growth strategy and meets all security requirements."

In short, the challenges facing the CISOs are many and varied, and the threat landscape seems to only grow and expand. However, with the right kind of leadership, it is clear that these challenges can be overcome and that businesses can stay a step ahead of their attackers. 🗝

cyber threats alone. "All of the teams need to work together and C-level executives responsible for data and technology must work together in order to stay secure."

According to Sam Curry, the role of the CISO/CIO varies by industry and the size of the company. However, the CISO is seen more and more as a risk management function — albeit technical in nature — rather than adjunct to IT. "It might not have started that way, but a CISO has more in common with

A NEW DIMENSION IN HOME SECURITY

MOHAMMAD MERAJ HODA, VICE-PRESIDENT OF BUSINESS DEVELOPMENT – MIDDLE EAST & AFRICA AT RING, ON WHAT IT MEANS TO PARTICIPATE IN GITEX THIS YEAR AND HOW SECURITY IS INTEGRATED INTO THEIR PRODUCT OFFERINGS.

What does participation at GITEX mean, this year?

GITEX Technology Week is really important for companies like Ring in developing markets as it allows us to meet with key decision makers and to inform the market on the areas we focus on. We would like to continue to build this momentum by participating in GITEX this year as well. It gives us an opportunity to showcase our innovations in the smart home security space and reiterate our message around neighborhood safety.

What are the products you'll be showcasing at GITEX?

At GITEX 2021, we plan to showcase our latest suite of smart home security products, which includes our latest Video Doorbells and Cameras - all Wi-Fi enabled and equipped with HD video, motion-activated alerts, two-way talk, and night vision. We plan to place the spotlight on our newly launched Video Doorbell Wired as well as our Stick Up Cams and Indoor Cam.

What is the demand for smart home automation products like, today?

Homes are getting 'smarter' with connected products offering endless possibilities to make our lives easier, and more convenient and comfortable. Safety and security are important. More and more homeowners are taking precautions to keep their homes safe and secure and protect their families and property. Homeowners

MORE AND MORE HOMEOWNERS ARE TAKING PRECAUTIONS TO KEEP THEIR HOMES SAFE AND SECURE AND PROTECT THEIR FAMILIES AND PROPERTY.

have also realized the convenience that smart home security can provide when they can see and speak with visitors from anywhere. Ring strives to give customers the peace of mind that comes from knowing their homes are more secure.

What is Ring's strategy for growth in a highly competitive market?

We have seen a strong traction for Ring in the Middle East region and this trend is continuing to grow. Our plan is to expand our regional footprint further by making our products more accessible in Middle East and Africa by engaging the right value-added partners, investing more in markets like UAE, Saudi Arabia, Bahrain to name some, where we have already strong presence. We are also adding a new line-up of products that will complement our current offering as well open new opportunities in different target verticals.

How do you make sure security is integrated into your product offerings?

At Ring, security, privacy, and user control are foundational. We are constantly innovating both our existing products and creating new ones to address various home security challenges. We have included a mandatory two-factor authentication, which adds an extra layer of protection. Ring also provides login notifications, which let you know if a new device logs into your account. Even though the company provides its customers with these extra security measures, at the same time it's important to boost your own security and have the most secure network passwords and account. Recently, we announced the end-to-end encryption, which is the latest in

the evolution of Ring's security and privacy features that gives users control and additional choices for encrypting and decrypting their videos. It is designed so that no unauthorised third party can access user video content. 🔒



Mohammad Meraj Hoda

DAWNING OF A NEW ERA DIGITAL TRANSFORMATION WITH INTELLIGENT AUTOMATION

ZAIDOUN ARBAD, COO, STARLINK TALKS ABOUT HOW BUSINESSES ARE TRANSITIONING INTO THE NEXT PHASE OF DIGITAL TRANSFORMATION WITH INTELLIGENT AUTOMATION.

The evolution of Digital Transformation post the pandemic

The main driver for organisations to prioritise Digital Transformation (DX) post the pandemic was to ensure business continuity, maintain a competitive edge and most importantly to enhance customer experience. Majority of the B2B organisations started their digitisation project plan three-to-five-years prior to the pandemic. However with the onset of the pandemic they were pushed over the technology tipping point that transformed businesses forever and were forced to accelerate their digital adoption at a dramatic pace covering anything related to remote working and virtual workplace with emphasis on securely accessing applications hosted on the cloud.

Challenges faced by enterprises in the DX journey

With this evolution in technologies and situational occurrences, businesses – big and small had to transform themselves into digital enterprises and focus on how to take the DX journey forward that would inculcate a mindset of continuous improvements and innovation with long term benefits in mind. To be successful, organisations were required to have the right set of tools, right expertise, and guidance to drive best results. Organisations that preferred to stick to the traditional operational methods found it

challenging to match the pace of digital transformation. While the ones fiercely adopting digital transformation stayed longer in the game and are today recognised as leaders.

Fast-tracking DX journey with Intelligent Automation

As per Gartner 91% of organisations are already engaged in some form of digital initiative. Digital Transformation emerged from the need to become agile, optimise productivity and deliver value. So, what's next? Organisations are expected to continuously adopt advanced technologies to keep up with the competition and respond to the market demands especially in a market where customers are expecting a digital-first experience. Therefore, it become imperative for businesses to keep 'Automation' at the core of any DX strategy and leverage on the latest technologies to deliver faster, better experiences at minimal cost.

Banking and Finance was one such sector that is predominantly process oriented which took to digitisation and realized that a shift in the culture that embraces innovation was inevitable. At this stage, we saw large enterprises evolve into the next phase of digital transformation with Intelligent Automation where they introduced robotic process automation (RPA) and artificial intelligence (AI) to automate complex end-to-end processes.



Driving value with StarLink's IA ecosystem

With StarLink Intelligent Automation, we aim to empower enterprises looking to build an automation-led digital transformation program with advanced technologies powered by Artificial Intelligence (AI) and automation to achieve increased productivity at reduced cost, greater accuracy, and improved customer experience.

Onboarded a holistic Intelligent Automation ecosystem that covers

- ✓ Intelligent Process Automation
- ✓ Intelligence Content Capture
- ✓ Intelligent Autonomous Digital Platform Automation
- ✓ Artificial Intelligence & Machine Learning
- ✓ Intelligent Data Automation and Data Science Automation
- ✓ Advanced Data Cloud Management and Master Data Management

From Robotic Process Automation (RPA) to Artificial Intelligence (AI) to Advanced Analytics, StarLink iA ecosystem can enable advanced automation and help organisations unlock new possibilities for higher operational efficiency and business success. Early adopters are already reaping great benefits.

'StarLink Transforms with Intelligent Automation', the

theme for 2022 is aimed at assisting customers revolutionise their business operations by securely incorporating intelligent technologies to become agile and resilient. This innovative approach will help reimagine business processes and accelerate growth:

- ✓ Enable enterprises customers across different business verticals to speed up their digital transformation journey.
- ✓ Reduce costs by augmenting the workforce and improving productivity
- ✓ Improve accuracy through consistent processes and approaches to enhance quality
- ✓ Improve customer experience
- ✓ Address compliance and regulations with confidence

With StarLink Intelligent Automation, our mission is to bring in best-of-breed technologies driven by Artificial Intelligence and Machine Learning to help enterprises across the different industries boost their efficiency, control costs, and achieve true digital transformation. 🔑

For more information: <https://www.starlinkme.net/iautomation>



DEV MEHTA

DIRECTOR, INTERNATIONAL MARKETING AT VIRSEC

What do you like most about a career in marketing?

Marketing is one of the strongest pillars of an organisation's growth. What fascinates me the most about marketing is the creative exposure that allows one to innovate and, with today's modern marketing tools, quantify it into measurable outcomes that contribute to the larger organisational goals. Marketing is all about creating a brand, a legacy that is sustainable and continuously yields results for the organisation.

Tell us about a defining point in your career.

Ahh, there have been a few. But the career move that I am most proud of is the one I took during the pandemic. I had a stable marketing role with one of the leading global organisations and then an opportunity came my way to work with my current employer, Virsec, a cybersecurity startup, which was looking to grow in the international market. I saw this position not only as an amazing learning opportunity, but also as an incredible chance to help create what I mentioned earlier -- a brand, a legacy. The organisation has a fantastic goal to make

Cyberattacks irrelevant. With our innovative solution, I can't envision a better story to be a part of then making the world a safer place to do business and building a more secure environment for nations against attackers. It was a defining moment when I had a call with my current CEO and he said, "Dev, we are on a mission and are you fully onboard?" My answer was an instant YES! A career is only as good as the risks you have taken and the stories you make, be it of success or failure, It's all about reinventing, redefining and being deterministic and true to your goals.

In your opinion, what are some of the most important qualities that a marketing professional should have?

Being Bold: It's important for marketers to shun silos and be open to new creative thoughts, ideas and be bold. It's ok if you fail, but that's the beauty of being a marketer -- it's all about bringing innovation, a bold attitude and a commitment to make a difference to the role.

Being Analytical: In the world we live in, everything has to drill down to Return on Investments (ROI) and marketers should be Analytical. It's great to try new campaigns, activations, and strategies, but it is equally

important to measure the outcomes. With all the intelligent marketing tools out there, it's becoming simple yet complicated and hence a 360 analytical approach is important.

Long term mindset: I am a cricket fan and I like to make the analogy that marketing is not for T20 or one day players but rather it's like a test match. It's a long game -- sales cycles can be long and you might have a bad day today or a good day tomorrow. But if you are consistent and optimistic, and have a focused team approach, you can contribute to the larger goal every day and, in the end, be victorious.

What does the leisure/weekend mean to you?

A leisure weekend for me means wandering to a nearest undisclosed location in the lap of nature for a trek, hike or just feeling nature in all its glory. I am a Musafir by heart and the journey never stops!

Three things you absolutely cannot do without, and why?

My sanity and strength, My family

Food, I am big foodie and love trying new cuisines that make me travel the world.

Music, It allows me to think, be creative and set a zone. 🎵

STARLINK

TRUSTED CYBER & CLOUD ADVISOR

TRUE VALUE-ADDED DISTRIBUTOR



STARLINK

TRANSFORMS

WITH INTELLIGENT AUTOMATION



Meet us at Hall 1 (H1-C1)
DUBAI WORLD TRADE CENTRE | 17 - 21 OCT, 2021

info@starlinkme.net
www.starlinkme.net



Protect Your Software as it Runs.

To fully protect your software, you must first fully understand it. Only Virsec can do this, by creating a dynamic golden image of what your software is supposed to do—and immediately stop anything that it's not.

NO

Dwell-Time

NO

False Alerts

NO

Learning, Tuning, or Noise

Stop Fileless Memory Attacks | Protect Legacy Applications |
Reduce Patching Urgency | Engineered for Servers—Not Endpoints

“We are at the inflection point for the next paradigm shift in cybersecurity and Virsec does what is needed: protect application workloads at runtime. This is the new battleground.”

– **John Chambers**, Virsec Investor and Strategic Advisor and Former Cisco CEO



We invite you to learn more: virsec.com | info@virsec.com