





THE FUTURE OF WI-FI

Wi-Fi 6 brings next-generation Wi-Fi technology into your home, giving the quantum leap in capacity, speed and range you need to handle all your Wi-Fi demands. Perfect for high-performance, device-dense smart homes.



DIR-X3260 AX3200 Wi-Fi 6 Router



DAP-X1860 AX1800 Mesh Wi-Fi 6 Range Extender



DIR-X1860 AX1800 Wi-Fi 6 Router













CONTENTS

Security











12

FRONTRUNNERS

March is the month for women. On this occasion, we celebrate the leading ladies in the field of cybersecurity and bring you their stories.



16 NEWS

News roundup from the cybersecurity industry in the region and beyond

- Dave Furneaux, CEO of Virsec, about his company's mission to create a movement of security partners that work together to make cyberattacks irrelevant, stressing that the current situation is now out of control.
- Ram Vaidyanathan, Product Manager at ManageEngine, on why CASB is a key tool in preventing data leak and providing more visibility for shadow applications.
- Demes Strouthos, General Manager at ESET Middle East, on the company's presence at GISEC and the products and solutions it is showcasing at the event.



Be data ready.

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

commvault.com



EDITORIAL



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

Anita Joseph Editor

EVENTS





POWER-PACKED

March 2022 is a power-packed month. Not only is it the time of year that celebrates women around the world for their strength and incredible presence, this year, it's also the month that hosts GISEC, the Arab world's largest security exhibition and conference that brings together Infosec and tech and change makers for three days of information & learning.

Echoing this mood, this issue of Security

Advisor is also a celebratory one: It pays story of h
tribute to the women in security whose one of the
vision and farsightedness are redefining the
industry globally, and it also
puts the spotlight on the

puts the spotlight on the three-day GISEC extravaganza which promises to be exciting, inspiring and game changing.

Our cover story is all about women power and how they are slowly but surely changing the face of the security industry. Featuring our pick of women cybersecurity professionals, the feature is a story of their journey through the ups and downs of their career. It is also a story of grit, strength and resilience against all odds. We're sure that this feature will inspire and move you, as it did our entire team.

Our other interviews are also rich and

varied: we have Mohammed AbuKhater, Vice-President, Middle East, Turkey & Africa at F5 tell us why application security is key to a robust defence against attacks. Ram Vaidyanathan, Product Manager at ManageEngine, points out why CASB is a key tool in preventing data leak and providing more visibility for shadow applications. Ammar Enaya, Regional Director – METNA at Vectra AI, tells us the story of how Vectra has evolved to become one of the most mature, hi-fidelity AIs in the market. Not to be missed is the special

interview with Dave Furneaux, CEO of Virsec, about his company's mission to create a movement of security partners that work together to make cyberattacks irrelevant,

stressing that the current situation is now out of control.

Don't forget to check out our GISEC special report featuring some of the trendsetters in the security industry. The products and solutions they have on offer are mind-boggling and is a great indication of the direction this industry is all set to take.

So enjoy this issue, we promise you a thrilling ride. Happy Reading!

FOUNDER, CPI Dominic De Sousa (1959-2015)

Published by



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

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.joseph@cpimediagroup.comm

OnlineEditor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

PRODUCTION AND DESIGN
Senior Designer
Analou Balbero
analou.balbero@cpimediagroup.com

Adarsh Snehajan
webmaster@cpimediagroup.com

DIGITAL SERVICES

Web Developer

WOMEN IN

SECURITY

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

Tel: +971 4 5682993

© Copyright 2022 CPI All rights reserved

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

PALO ALTO NETWORKS HELPS ORGANISATIONS COMBAT SOFTWARE SUPPLY CHAIN THREATS

ANKUR SHAH

With software supply chain attacks rising rapidly, Palo Alto Networks has



announced Prisma Cloud Supply
Chain Security to provide a complete
view of where potential vulnerabilities or
misconfigurations exist in the software
supply chain — allowing organisations to
quickly trace to the source and fix them.
If not quickly fixed or, better yet, avoided
during coding, these security flaws could
allow attackers to infiltrate systems,
spread malicious payloads throughout
an organisation's software and access
sensitive data.

According to Gartner, "By 2025, 45% of organisations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021." Unit 42's Cloud Threat Report also found that access to hardcoded credentials opened the door for lateral movement and continuous integration/continuous delivery (CI/CD) pipeline poisoning.

"Every day new vulnerabilities are found in open source and other software components that have previously been integrated into the organisation's software code. Without the proper tools, it is very difficult for organisations to quickly spot where they have used the unpatched versions of these components," said Ankur Shah, senior vice-president, Prisma Cloud products, Palo Alto Networks. "Prisma Cloud is designed to help protect organisations from code to cloud; and now that customers can visualise their software supply chain, it's easier to spot, prioritise, and remediate security weaknesses at the onset of development and during delivery pipelines."

ESET RECOGNISED AS A TOP PLAYER IN RADICATI'S APT PROTECTION MARKET QUADRANT FOR THIRD

YEAR IN A ROW

ESET, a global cybersecurity leader,

has been recognised as a Top Player for the third year in a row in Radicati's 2022 Advanced Persistent Threat (APT) Protection Market Quadrant. The report evaluates 10leading security vendors for their APT Protection solutions, particularly assessing their functionality and strategic vision, with ESET's Top Player status signifying continued excellence in this field.

APT Protection solutions include in ESET's case, solutions such as an XDR-enabling enterprise management platform (ESET PROTECT Enterprise), advanced threat defense (ESET LiveGuard Advanced), endpoint detection and response (ESET Inspect), reputation networks (ESET LiveGrid®) and threat intelligence (ESET threat intelligence feeds and APT reports).



Jakub Debski, ESET's chief product officer, said: "ESET's prevention technology is the most densely multilayered and effective in the industry and we've created a wealth of diagnostic systems to detect and halt malicious code. Altogether they work as an extended detection and response, or XDR, solution that delivers enterprisegrade security and risk management capabilities, including advanced threat hunting, incident response, full network visibility, cloud-based automated threat defense, and more."

INFOBLOX OPENS UP THREAT RESEARCH AND DNS SECURITY SERVICE

Infoblox Inc., the leader in DNS

management and security, is committing its top threat intelligence to GitHub to share its most relevant research with the broader security community as the invasion of Ukraine has placed organisations around the world on elevated alert for cyberattacks.

Already, Infoblox's threat researchers have reported on three separate campaigns that weaponised the crisis in Ukraine to deliver malware infections (Agent Tesla and Remcos) and financially fleece well-intentioned people. These fast-moving cyber campaigns prompted the company to share its threat intelligence in the form of machine-readable files that make it easy for defenders to integrate threat data into their systems. Today, Infoblox's GitHub repository contains over 800 indicators, including malicious and

CRAIG SANDERSON



suspicious domains, as well as legitimate domains that might be blocked by other vendors through automated analytics.

Detailed information is available to Infoblox customers in the Threat Indicator Data Exchange (TIDE) database.

"We're committed to doing what we can to protect organisations from cyberattacks," said Craig Sanderson, VP of Product Management, Infoblox. "The escalating risks require that we collectively help critical infrastructure, supply chain vendors, and other potential targets defend themselves. This is also why we are bringing product enhancements, like more granular threat feeds, and free access to BloxOne Threat Defense to bolster customers' cyber arsenals."

SAFE SECURITY BOARD WELCOMES CYBERSECURITY VETERAN

Safe Security, a global leader in

Cybersecurity and Digital Business Risk Quantification, announced the appointment of Michael Johnson, a veteran US government and commercial industry Chief Information Officer (CIO) and Chief Information Security Officer (CISO), to its Board of Directors. Johnson has been advising Safe Security since December 2020. Michael joined the Board of Directors of the company on November 10, 2021.

"We are delighted to welcome Michael, a veteran in cybersecurity to the Safe Security Board," said Saket Modi, Co-founder & CEO of Safe Security. "Michael's experience in managing cybersecurity for government and large organisations in the US is indispensable. His expertise in building and executing cybersecurity strategies, coupled with his deep understanding of cyber is extremely valuable for us as we grow and

MICHAEL



expand to achieve our mission to become the defacto industry standard to measure, manage and mitigate cyber risk."

Johnson currently serves as CISO, Meta Financial Technologies, Meta Platforms, Inc., and previously served in multiple cybersecurity roles leading large, complex, and dynamic information-intensive global enterprises, including as the Senior Vice-President and CISO at Capital One, the CIO for the U.S. Department of Energy, and in other key roles in the Executive Office of the President (the White House), the U.S. Department of Homeland Security, and the Office of the Director of National Intelligence.

SANS INSTITUTE TO HIGHLIGHT INTERACTIVE CYBERSECURITY TRAINING AND WORKFORCE DEVELOPMENT AT GISEC 2022

SANS Institute, the global leader in

cybersecurity training and certifications, has announced its participation at GISEC 2022, to be held at the Dubai World Trade Centre, from March 21 to 23. At the event, SANS will showcase a vast range of their offerings, from core training courses, Capture-the-Flag events (CTFs), security awareness products, knowledge assessments, NetWars tournaments and Cyber Training academies, to educate visitors on how SANS can support organisations in training, recruiting, and retaining cybersecurity staff.

"There is an ever-growing cybersecurity skills gap and need for trained personnel within organisations. With a growing shortage of people available on the job market, it is becoming increasingly challenging for

NED BALTAGI

organisations to find the right talent for the right jobs," said Ned Baltagi, Managing Director, Middle East and Africa at SANS Institute.

"We have many products to offer organisations – small and large – to help them provide their staff with the best possible training experience. As the largest and most anticipated cybersecurity exhibition in the Arab region, GISEC is the best platform to spotlight our larger product portfolio and inform professionals that SANS' proficiencies expand beyond our training courses," Baltagi added.

VIRSEC TO HIGHLIGHT NEW DETERMINISTIC PROTECTION PLATFORM AT GISEC 2022

BOBBY GUPTA



Virsec, the

first cybersecurity company to fully protect software as it is running, has announced its participation at GISEC 2022, where it will be showcasing its recently launched Deterministic Protection Platform (DPP). DPP is the next evolution of the company's flagship and award-winning Virsec Security Platform (VSP), the first solution that could eradicate threats to the software workload at runtime in real-time.

"As the largest, most anticipated cybersecurity exhibition in the Arab world, we want to highlight and share our progress at GISEC," said Bobby Gupta, Senior Vice-President and MD of International Business at Virsec. "During the pandemic, we all have witnessed a surge of increasingly sophisticated cyberattacks, and the rate continues to grow. Organisations are now in need of a solution which can protect both known and unknown vulnerabilities from being exploited - a solution which does not only detect with extreme precision, but also automatically protects – without human intervention "

"With DPP, Virsec can establish a stronger foothold in the Middle Eastern market, and we plan to invest in and provide the best in-class cybersecurity to customers in the region. We are also looking forward to welcoming our CEO, Dave Furneaux, who will attend the conference this year, where he will engage with key customers and partners," Gupta added.



interview opportunity with the charismatic American, and we began our conversation by going back to the beginning and finding out the purpose and vision behind the inception of Virsec.

Furneaux stressed that the company was established out of a necessity to find a protection capability that equipped businesses with the security they needed to better protect their IT environments.

"Virsec is a very atypical cybersecurity company, and when I say it is an atypical company, I say that because the company was founded on a question of what do we need to do to really work on a new protection capability that will be stronger in the marketplace and allows companies, governments, and militaries to be more fully protected? It was a very provocative question that we started the company on, and it led to several years of working on the technology," said Furneaux.

He disclosed that Virsec have 113 patents and many trade secrets around their body of work and said that it ultimately led them to a first-principle way of thinking, and illustrated how important it was to better understand the software at play when attempting to protect it.

"What a first principle way of thinking essentially means if you apply it is thinking about complicated problems, and we had to break the problem down into its most basic form. In the world of digital it means you are breaking the problem down right in to the software, and you're saying that we have got to figure out and fully understand the software that needs to be protected if we are going to fully protect it. We spent 3 years building this technology,

and then we spent a year testing it - and it was two years after that we came to market with the product. We really learned in 2020 with about 10-12 customers what it needed to look like, how does it need to work and where does it need to go – and then last year we really started to figure it out, and we are now starting to scale the business out globally," said Furneaux.

Virsec have been an advocating for a deterministic approach to tackling cybersecurity problems versus the seemingly preferred probabilistic model being pursued by the industry. However, Furneaux stressed that Virsec is coming into market very humbly and is looking to complement the existing processes.

"Virsec isn't coming into the market saying we are here now, so you don't need the other things, that's not the case at all. We want to complement today's security programs and fit into their customers' existing security stack, and then over time the customer will undoubtedly see the ways in which they are getting efficiency out of this new protection approach because it automates, it is precise, and it is all

"VIRSEC ISN'T
COMING INTO THE
MARKET SAYING
WE ARE HERE NOW,
SO YOU DON'T NEED
THE OTHER THINGS,
THAT'S NOT THE
CASE AT ALL."

done in real-time," said Furneaux.

The CEO of Virsec then explained the differences between a probabilistic and deterministic approach.

"If you break down the word probabilistic then it means probable. We've built an industry on detection and response, and right in the middle there is that word probable. We are analyzing data coming from the infrastructure and the software and we are trying to determine if an attack is occurring by detecting it in a probabilistic way, so we are probably protecting it, but we don't know. Then we are trying as quick as we can to respond to it, so the response part is threat hunting, but during the hunting process the damage is already done and that's what we call dwell time. Virsec comes in and we use the word determine, and our function is to determine whether the software that you want to protect is doing what it is intended to do and assure the security leader that the software is only doing what it was intended to do," said Furneaux.

Furneaux detailed the gains of this approach and highlighted that another attractive characteristic of their deterministic model is that fact that enterprises don't need to radically transform their operations to implement their solutions, but instead can integrate it in small stages.

"The benefits and gains are better protection, automated protection, and no need for full-time people managing the tool. In summary, we are coming in to complement the existing environments, and we've worked very hard at trying to make that as approachable and easy as possible for companies to bring it in, so they don't need to make wholesale changes. They



can start small and grow in confidence, and use the product more over time," said Furneaux.

Virsec have recently received capital investment to the tune of \$100m, but more significant is who the capital has been raised from.

John Chambers and Mike Ruettgers, two titans of the IT industry have given Virsec a ringing endorsement with their investment into the company, and as Furneaux revealed both are fully committed to helping Virsec achieve their mission statement.

"I see Virsec more like a movement. Yes, we are a company that is building a product and are solving a problem, but what we really want to do is encourage the industry to move in a first principle way towards protection. We would love nothing better than for all the major security companies to move in this direction too, because our mission is to help solve this problem, and gain more

control out of the infrastructure we have today, because quite bluntly speaking it is out of control, and we can see that every day. In relation to building the company you need capital as fuel to grow and scale - and make the right investments to mature the product and simplify how you come to market. We chose very carefully who we wanted to raise the capital from to support our mission. John Chambers is one of the leading businesspeople of the last generation in building Cisco into such a dominant company. Mike Ruttguers came into EMC as a small company and built it into a billion-dollar company as the CEO, and he is now on our board. Both these gentlemen work with me on a day-to-day basis. We also went beyond that and built a growth advisory board of CIOs and CSOs, congressman and former CIA directors, and this group of people have accelerated and unlocked our growth and are on that mission with us to make cyberattacks

irrelevant." said Furneaux.

The second ever customer of Virsec was based in the Middle East, and Furneaux revealed that the company has ambitious aspirations in the region, and firmly believes they are well placed to become the go-to protection player in the region over the next 5 years.

"The Middle East is one of our priority regions. Early in the rollout of our product our second customer was based in the region, so that serves as a testament to how important a market it is for us. We have started selling more broadly in the Middle East, and we have spent the last two years building proof points and selling into five different countries, but with a real focus on the quality of engagements with the right partners. We are now at the point where we want to make an investment over the next 3-5 years to become the dominant protection capability provider in the region," said Furneaux. 1



The Region's Finest IT Distribution Company for globally renowned brands

NEWCOM is one of the leading IT distributor companies offering Enterprise as well as Consumer solutions catering to information technology which includes Tech Accessories, Security Solution, Display & Video Conference Solution. With our current presence since mid-2021 in Africa region, we have opened our doors for new brands under new categories to associate with our growing team.



TECH









Authorized Distributors

SAMSUNG · HIKVISION · logitech ·







norton · rxpoo · V ·







@newcommea

#absolutelygenius



FRONTRUNNERS

MARCH IS THE MONTH FOR WOMEN. ON THIS OCCASION, WE BRING YOU OUR PICK OF THE LEADING LADIES IN THE FIELD OF CYBERSECURITY. WITH THEIR VISION, RESILIENCE, DRIVE AND COMMITMENT, THESE WOMEN HAVE CARVED A NICHE FOR THEMSELVES IN A HIGHLY COMPETITIVE SPACE. READ ON TO FIND OUT HOW THEY NAVIGATE THE CHALLENGES OF THEIR ROLE AND WHAT THEY WOULD ADVISE ASPIRING CYBERSECURITY PROFESSIONALS. A SECURITY ADVISOR EXCLUSIVE.

omen have slowly but steadily been making their presence felt in the highly competive and challenging field of cybersecurity. In fact, studies show that women now make up approximately 20% of the global security payrolls. So it's not difficult to imagine how some of the most crucial decisions taken in this domain have been driven by women-how their astuteness, farsightedness and remarakbale vision have contributed to positive changes in the way we approach today's highly complex threat landscape. Let's hear it from the leading ladies who are fast changing the cyber defence landscape of the world.

OFTEN, COMPANIES
OVERESTIMATE HOW
ROBUST AND SOLID
THEIR SECURITY
POSTURE IS WHEN IT
CLEARLY ISN'T."



Ciara Campbell, Senior Security Engineer, Tenable

As a Senior Security Engineer at Tenable, Ciara's role can be quite varied, but the customer is always at the heart of everything she does. "My role is to consult with customers to help them identify their challenges, concerns and obstacles securing their business whether it's on premise or in the cloud, utilise our products, our resources, and our team's knowledge to enable our clients to achieve their cybersecurity goals. We

like to think of ourselves as an extension to their team and customers having trust in us is hugely important. There is satisfaction in a customer, particularly one who might be struggling, and I can help them solve their problem." she says.

According to her, keeping up with all the technical knowledge can sometimes be hard, particularly as the subject is so vast and attack paths evolving. I have learnt that everyone comes across things they haven't heard of before or haven't seen and it's okay to say "I don't know that, can you tell me about it".

An important lesson she has learnt is that there is no need to feel like you need to know everything. "I am very lucky to have worked with some great people who were willing to help and share their knowledge and more importantly not make you feel that your question is stupid. It's continuous learning every day," she adds.

Ciara's advice to aspiring women cybersecurity professionals is to do what you love and watch it all fall into place. "If you want to work in an exciting and fast changing environment with huge opportunities for growth then Security is the industry to be in. Even if you think the

technology is not up your street there are so many other jobs in this area that make it really exciting. I really feel people don't realise this, you could work in marketing, finance, legal, HR etc. It doesn't always have to be a technical position and you will still be excited about the industry and learn something new every day."



Debanjali Ghosh, Technical Evangelist, ManageEngine

As a cybersecurity evangelist, Debanjali's primary role is to garner awareness about potential threat vectors and provide actionable insights to technology leaders and decision-makers to build a cybersecurity blueprint tailor-made for their organisation. "Working with CISOs around the world has allowed me to understand their pain points, and I contribute strategic insights on deploying industry-recognised cybersecurity frameworks," she says.

Debanjali has a very focused approach to challenges. "The cybersecurity landscape is ever-evolving, so it's critical for me to stay on top of things. As technology evolves, threats become equally sophisticated. After the pandemic hit, there was a quantum shift to remote

work and an increase in unmanaged devices. While organisations struggle to keep the lights on, it's been challenging to get them to prioritise security over accessibility. Often, companies overestimate how robust and solid their security posture is when it clearly isn't. It's part of the job description to challenge their beliefs and help them see clearly. However, I also observe that in some companies, security is still an afterthought or there are budget constraints. Working with IT teams to get management buy-in for a thoughtout cybersecurity program has been challenging."

Her advice to women aspiring for a cybersecurity career: "As women, it's our innate tendency to protect. Listen to your gut and use your powerful intuition to identify patterns and come up with solutions. Take responsibility for the job and at the end of the day, it'll be empowering to know that you created an impact in making someone's walk of life a little more secure."



Layale Hachem, Senior Solutions
Engineer – BeyondTrust
Layale handles pre-sales activities for

THE ADVERSARY IS JUST AS INNOVATIVE AND AGILE AS THEY'VE ALWAYS BEEN, BUT THEY'RE ALSO MORE PROLIFIC."

BeyondTrust — the worldwide leader in intelligent identity and access security — across Qatar, Kuwait, Oman, Bahrain, Egypt, and North Africa. "As part of my job, I spend a lot of time understanding customers' cybersecurity strategies and gaps and working closely with them to deploy our advanced privileged access management (PAM) solution, in order to protect all privileged identities, access, and endpoints, across an organisations' IT environment, from security threats," she says.

In her own words: "A positive approach to challenges is the best strategy one can use to overcome obstacles. While some situations can be upsetting, I try to remain logical and tackle problems systematically, until resolved. I also acknowledge the fact that challenges are a normal part of any job and that one must have the determination to overcome them and should also be wise enough to seek help when required."

In her opinion, the time is right for women to make their mark. "We as women might feel like we don't fit it in a male dominated industry, but the truth is technology, and particularly cybersecurity, is the perfect place for us to shine and prove that we have what is takes to be successful and a very important resource to the business."



Maysa Salameh, Regional Channel Manager – Middle East, Infoblox

Maysa runs the regional channel business for Infoblox in the Middle East (Saudi and Levant). As a channel manager, her goal is to increase channel coverage for Infoblox and strengthen partners with the right tools and training. "I am working to enable partners to act as an extended arm for Infoblox in the market by enhancing their capabilities and thereby driving growth for our company through them," she says.

According to her "cybersecurity has evolved over the past few years. Significant shifts and transformations have occurred, and we expect similar rapid changes and new innovations and trends to come. The greatest challenge is to stay up to date with the dynamism of the technology industry."

Maysa believes that the cybersecurity industry has come a long way in a short time, and that it is not male-dominated anymore. "Women have proven themselves and are making a positive impact in their organisations and getting equal opportunities. I encourage women who aspire to believe in themselves and look towards their dreams and never give up. I always say great minds dream big. If you

are a woman in the technology field, be loud and proud about it. Be bold and take the first step to where you want to see yourself in future."



Michel Huffaker, Director, Threat Intelligence, ThreatQuotient Michel is the the Director of Threat

YOU DON'T HAVE TO EMBRACE ALL CHANGE, BUT YOU MUST HAVE A BROADER VIEW OF THE BUSINESS PROBLEM, INCLUDING UNDERSTANDING GEOPOLITICAL ARENAS AND THE GLOBAL MARKET IN WHICH YOU PLAY."

Intelligence at ThreatQuotient. Her role here involves managing and executing consulting, training, and implementation professional services. "I've been in the cybersecurity industry for over 12 years now, and I love how dynamic it is," she says. "I've had so many high points in my career, it's difficult to point to just one, but I take great joy in seeing other companies succeed in defending themselves against the litany of attacks that plague them. That is particularly rewarding as a trainer and consultant because I know my team has made real progress towards making the world a safer place online," she adds.

In her opinion, most of the challenges in this career field involve staying educated about adversaries and their tactics. "The adversary is just as innovative and agile as they've always been, but they're also more prolific. So, there's an almost constant need to study available threat intelligence. My approach to keeping up with this is to subscribe to reliable intelligence sources, join webinars about new technologies, and spend as much time (even virtually) talking to the intelligent people dealing with these issues daily," Michel points out.

According to her Women know we can succeed in the cybersecurity field, but sometimes they must convince themselves as much as those around them. "I owe much of my success to a continuous drive to be heard and to have a seat at the table. There will be times when it feels uncomfortable to speak up because maybe it's not how things usually work, but it is worth it. Cybersecurity is a dynamic field with evolving challenges. It requires a diverse group of people working together to make progress. You are part of that diversity."



Mor Levi, VP, Global Security Practices, Cybereason

Mor is the VP of Global Security Practices at Cybereason. As part of this role, she leads a global organisation of cybersecurity experts that are responsible for providing Incident Response Services, Threat Research & Intelligence.

In her words, "the cybersecurity industry is exciting and challenging at the same time as adversaries are well-funded, patient and motivated. My biggest focus is working with co-

SUPPORTING AND UNDERSTANDING THE CHALLENGES THAT REGIONAL BUSINESSES FACE ON A DAILY BASIS ARE KEY WHEN WORKING IN CYBERSECURITY."

workers on a daily basis to make sure our customers are safe and secure. I tend to overcome challenges by looking at the glass being half full, am patient with co-workers and understand that we all make mistakes but most of the time there is no malicious intent."

In her opinion, no matter what industry you aim to be part of, is to believe in yourself and your abilities. "Never spend your energy and time in environments where people don't appreciate you and your contributions. Not only is it unhealthy but it isn't sustainable for long periods of time and will lead to undue stress and anxiety."



Nadia Zamouri, Territory Manager -META, Delinea

Nadia joined Delinea (then Thycotic) over four years ago with the remit of establishing a solid foundation for the company in the META region by building a new local team, raising brand awareness, developing a network of qualified partners and growing the company's customer base. Having successfully achieved these objectives,

today her role has evolved into the management of Delinea's largest clients in the region and nurturing long-term partnerships to ensure these clients understand our value proposition and that projects are successfully implemented.

In her opinion, "supporting and understanding the challenges that regional businesses face on a daily basis are key when working in cybersecurity – and I firmly believe that being part of that journey and contributing to the long-term strategies of organisations are key components of building long-term partnerships with clients and partners."

So, how does she stay ahead of challenges? "Passion, Determination and Persistence! Passion is what drives me to wake up every morning and go to work with an incredible team that works hard and helps our customers overcome their security challenges day in and day out. It is this passion helps me enjoy my work and drives me to perform at my best not only for myself, but also for customers, partners, and colleagues."

Her advice to all the women aspiring to work in this industry: "Do it – get the support of your peers, and seek that seat at that table by showcasing your strengths, results, and values. I would also recommend they consider joining 'Women in Cybersecurity Middle East,' a voluntary group which has a vision of building 'a strong, dependable, and increasing network of passionate female cyber security professionals in the Middle East and African countries' and has already scaled to over 300 members."



Sandra Hattab, Cybersecurity Consultant, Axon Technologies

Sandra prides in being part of a growing cybersecurity services firm, Axon Technologies, that partners with clients from around the globe as they work towards achieving cybersecurity goals across their value chain. "Cybersecurity is a fast-paced world with new trends emerging every day. With the evolvement of the digital world, customers face unique cybersecurity challenges that require tailored solutions to minimise and eliminate the risk of being compromised."

"To stay sharp, I have adopted the approach of the lifelong student.

Learning is a never-ending process.

Whether it is by reaching out to a colleague for brainstorming and problem-solving, learning on the job, or signing up for professional training, I know these challenges can always be conquered," she adds.

According to her, while it's easy to pick an area of focus that suits a person's career aspirations, "I invite you to challenge yourself by taking on roles that cover different areas of cybersecurity and to be ready to go the extra mile learning from cross-functional and critical assignments. This is key to gaining a well-rounded cybersecurity experience. I also advise you to get a mentor that can help you navigate your career and growth options in the field of cybersecurity."



Tina Stewart, Vice-President of Global Marketing, A10 Networks

Tina's security career spans operations, product marketing, business development and digital marketing in companies such as Network Associates. Having led startups and global teams, Tina has developed messaging for service providers and enterprises that spoke to CISOs' needs on topics, like DDoS protection and encryption, making security approachable while also being seen as a business enabler versus an inhibitor. "With this experience. I created Juniper Network's social media program to engage directly with CISOs on topics beyond security. As part of my team's maniacal focus on the customer, I drive digital transformation programs, creating a more customised experience all around."

According to her, being aware of changes and embracing them is critical. "Let's take the metaverse, for example. You don't have to embrace all change, but you must have a broader view of the business problem, including understanding geopolitical arenas and the global market in which you play."

Her advice to aspiring cybersecurity professionals: "There's so much opportunity right now for women. I used to be the only woman in a room full of executives. Then, at Network Associates, we had multiple female executives. It's important for women to have multiple mentors that both men and women engage regularly to have open conversations. When starting off, if you know 50% of the job required, take the extra leap and apply for it, while learning and growing into it. Trusting your ability to build your knowledge can address this gap. Take advantage of the many great podcasts available, along with reading industry and competitor news." 1

POWERED BY AI

AMMAR ENAYA, REGIONAL DIRECTOR - METNA AT VECTRA AI, TELLS ANITA JOSEPH ALL ABOUT HOW VECTRA IS ONE OF THE MOST MATURE, HI-FIDELITY AIS IN THE MARKET.



detection and response. Can you tell us more? You're absolutely right, Al is becoming an integral part of many industries. In cybersecurity in particular, AI is helping Vectra to automate threat detection. So. without AI, all the work that Vectra is doing, must be done manually. And as you know, doing manually also works theoretically. So if you don't have VECTRA or NDR or Al, you can still more or less achieve what we do, but you need to have a very good aggregator, very strong SIEM and a very focused SOC team that does not miss a single event, who can separate the noise from the threats as quickly

ectra is known for its Aldriven approach to threat

Attackers these days are quick, unpredictable and fast-they do the

damage in a few hours. So the faster you can put your finger on the attack and identify it, the sooner you'll be able to resolve it and stop it for good. This is the power of AI and we're not talking about any AI. Vectra is one of the most mature AIs in the market, because we started it like ten years ago. We're also claiming to be one of the highest Fidelity AI. We all know that with AI, fidelity is important-the higher the fidelity the better.

What are some of Vectra's latest products and solutions that address the growing threat and attack landscape?

Vectra evolved from a threat hunting platform to network threat analytics to network detection and response. We keep evolving. Vectra, traditionally, was the king of on-prem solutions and so those who were not very keen on the cloud, they liked Vectra. With time, we realised that people want automation of response and this is where the highfidelity aspect becomes important. Now, because we claim to be a highfidelity AI engine in detection, then it makes sense that you also automate response. This is where Vectra did a great job by partnering with market leaders in EDRs, firewalls, etc, so that we can automate the response.

Another thing which we introduced lately, specifically for the pandemic, is the cloud. Vectra started from an onprem master and now we are also cloud master. We have signed partnerships with Microsoft, so we have an NDR portion within the Azure for office 365 and it's a market leader product. It really does solve a lot of NDR concerns which will allow customers and help us get visibility within the office 365.

"ATTACKERS THESE DAYS **ARE QUICK. UNPREDICTABLE AND FAST-THEY** DO THE DAMAGE IN A FFW HOURS. **SO THE FASTER** YOU CAN PUT **YOUR FINGER** ON THE ATTACK **AND IDENTIFY** IT, THE SOONER YOU'LL BE ABLE TO RESOLVE IT **AND STOP IT FOR** G00D."

What's the cybersecurity landscape looking like in 2022 and beyond?

Unfortunately, the pandemic and recent war in Europe are posing greater risks to networks, mainly because threat actors have a much bigger space to operate in now, with remote/hybrid work gaining traction. So the cybersecurity teams in every organisation must work extra hard to ensure that their IT environment is compromise-free.

The minute you talk about compromise, you talk about compromise assessment. The

minute you talk about compromise assessment, you talk of NDR and Vectra. As you see, the need for an NDR is becoming more and more important. In the earlier day, NDR was good to have because if you have good prevention, you stop 99.9% of the noise. Now, with the pandemic, the attack surface is bigger so it's just a matter of time before somebody manages to hack into a network. There are many reasons that a hacker will manage to parachute into your network, bypassing all your prevention tools. So the last defence factor you have is visibility. And a very high-fidelity NDR like Vectra will give you near real-time or early alert visibility which will allow you to stop the attack before it does any damage.

How has Vectra been performing in the Middle East market?

Vectra has been in the Middle East now for a while.

It's gaining markets on a daily basis. Major government and private sector enterprises are all either deploying Vectra or converting from other NDR to Vectra.

They appreciate our availability in the market-we are in the Emirates, we are in Saudi, we are in Jordan, Egypt, Turkey. So we have high availability in all these countries. We also have strong partnerships here with key cybersecurity companies and key MSS partners -they chose Vectra to be their partner because they believe we deliver a good product and provide solid and reliable support to our partners and customers.

We expanding. Every quarter we add additional people on the ground. We are happy that our product is adding value to our partners and our customers. 1

BREAK THE BIAS AND CREATE A MORE DIVERSE AND INCLUSIVE CYBERSECURITY WORKFORCE

BARBARA MAIGRET, GLOBAL HEAD OF SUSTAINABILITY & CSR AT FORTINET

his year, on International
Women's Day, governments,
organisations, and individuals
worldwide were asked to
help envision and create a
gender-equal world. A world free of bias,
stereotypes, and discrimination. A world that
is diverse, equitable, and inclusive. A world
where difference is valued and celebrated.
That is this year's theme: #BreakTheBias.

One of the industries struggling with significant bias and gender stereotypes is cybersecurity. This field plays an increasingly crucial role in our digital world and, as a result, offers many fulfilling career paths and opportunities. However, there are still significant barriers and misperceptions driving the belief that a career in cybersecurity is not for women.

Women are underrepresented in cybersecurity

While women have been disproportionately impacted by pandemic-driven unemployment (for example, one in four women reported job loss due to a lack of childcare—twice the rate of men), the technology sector was less affected.

This was mainly due to their being better prepared to pivot to remote work and flexible work models. As a result, according to a report by Deloitte Global, large global technology firms still managed to achieve "nearly 33% overall female representation in their workforces in 2022, up slightly more than two percentage points from 2019."

While such progress is good, the technology sector still has a long way to go



compared to other industries. Outside of the high-tech sector, women account for 47.7% of the global workforce. And they also make up 50.2% of the college-educated workforce.

And the gender gap is even wider within the cybersecurity industry where, according to the (ISC)2 Cybersecurity Workforce Study, women only make up 25% of the global cybersecurity workforce. This gap is certainly not because there aren't any jobs. According to that same study, the cybersecurity industry urgently needs 2.72 million more professionals. And while 700,000 cybersecurity professionals entered the workforce in the past year, the global workforce gap was only reduced by 400,000, indicating that global demand continues to outpace supply. Women are just generally not applying for or being recruited to fill these positions.

This lack of gender equity has also directly contributed to the low percentage of women who hold cybersecurity leadership roles.

In 2021, for example, only 17% of Fortune

500 CISO positions were held by women, with only one female CISO in the top ten US companies.

Stereotypes and misconceptions persist

There are three main reasons why women continue to be underrepresented in the cybersecurity industry:

Problem #1: Cybersecurity is seen as a man's career

Many women don't consider cybersecurity a career path because it's primarily seen as a male profession. This image is reinforced by popular media, such as Eliot Alderson in the Mr. Robot TV series, where cyber activities are performed by young geeks in hoodies working late at night in a dark room lit only by their computer screen. While it may make for compelling TV, this stereotype is inaccurate and off-putting for many women, inadvertently contributing to gender disparity in the workforce.

While cybersecurity certainly has its technical aspects, it is not just a technical industry. Like any growing industry, there are a wide variety of job opportunities that require human skills. These include analytical, communication, management, and interpersonal skills that are equally important to the organisation's success and positively impact the industry.

Problem #2: Young women are underrepresented in STEM programs

One reason why so few women apply for cybersecurity positions is they are less represented in STEM-based programs.

But there is no reason why the technical aspects of a career in cybersecurity should be off-putting for women. Pervasive gender biases, few female role models, mistaken beliefs about technology being a maleoriented industry, and, sadly, teachers and parents who steer girls away from technology studies have combined to break the confidence of many young women otherwise suited to pursue a STEM-related degree. This is a global issue, with women generally earning less than 20% of all STEM degrees. This bias starts early in their college careers. 49.2% of women intending to major in science and engineering switch to a non-STEM major during their first year.

Problem #3: Bias in cybersecurity hiring

We cannot cure the lack of women in STEM overnight. So, organizations need to think differently about the composition of their cybersecurity staff. Many hiring managers—and HR—view individuals with backgrounds in computer science, engineering, and other STEM fields as the most qualified cybersecurity candidates, often ignoring those with degrees in other areas. But if they want to build successful cybersecurity teams, they need to broaden the scope of backgrounds they consider when looking for new employees.

But the challenge goes beyond hiring. The reality is that women in cybersecurity roles also tend to be promoted more slowly than men—something known as the "first rung" problem. According to Fortinet CISO Renee Tarun, "Men are four times more likely to hold executive roles than their female counterparts, they're nine times more likely to have managerial roles than women, and [on average] they're paid 6% more than women." In addition, women tend to leave the field at twice the rate of men, citing gender bias, discrimination, and harassment as their reasons for leaving.

Five steps for creating a more diverse and inclusive cybersecurity workforce

Given the rate at which digital innovation is transforming organisations (and the efforts of cybercriminals to exploit those digital acceleration efforts), now is the time to break our cybersecurity stereotypes.

We must work together to remove the bias that cybersecurity is a gender-specific field and change the perception that it is purely a computer science discipline. In cybersecurity, technology is only one of the silver bullets required to eliminate cyberattacks. The three critical elements of an effective cybersecurity strategy are People, Products, and Processes. But when we continue to recruit the same people—same gender, same educational background, same perspective—we are unlikely to develop strategies that allow us to get out ahead of our cyber adversaries. For example, it is not a stretch to say that the failure to rethink security strategies—starting with who makes up our cybersecurity teams—played a part in the nearly 1100% increase in ransomware attacks organisations worldwide experienced last year.

To change this perception and get out ahead of the cybercrime crisis we all face, we must bring more voices, perspectives, and diversity to our cybersecurity teams. Here are five basic principles we need to adopt as we work to refine our cybersecurity teams and strategies:

Highlight the contributions of women in cybersecurity in our classrooms and businesses, identify and promote positive role models and examples, and actively encourage diverse career paths, experiences, and job functions to our young women.

Encourage young women to pursue STEM-based degrees and careers at a young age.

Create and/or be part of mentorship programs at all levels, beginning with basic technology classes in elementary schools

MANY WOMEN
DON'T CONSIDER
CYBERSECURITY
A CAREER PATH
BECAUSE IT'S
PRIMARILY SEEN AS A
MALE PROFESSION.

that model success in technology for girls that continues throughout their higher education and professional careers.

Implement more inclusive work environments by identifying and breaking bias in hiring practices, training all employees (not just executives) about true inclusiveness, and actively making every employee feel involved, valued, and respected. And we need to ensure that women, especially women of color, are treated fairly and are fully embedded in the workplace.

Eliminate "first rung" barriers by actively promoting more women to leadership at every level of the organisation, beginning with roles as project and team leads and first-tier managers.

This must be a commitment we are all willing to make. On this day, we reaffirm our commitment to promoting gender diversity, equity, and inclusion inside Fortinet by helping engage more women in the cybersecurity sector through concrete action across the above strategies.

Final Thoughts

Cybersecurity plays an essential role in our modern society. However, a variety of skills and experiences must come together to guarantee the cyber industry's success. And as with any other industry, diversity is crucial. By bringing greater awareness to the diverse skills and backgrounds cybersecurity requires, we can help shrink both the gender and skills gaps while making strides in our battle with our cyber adversaries.

Cybersecurity offers many fulfilling career paths and opportunities for women. Because technology—and cyberthreats—continue to accelerate, it is an industry in constant evolution, making the field of cybersecurity very stimulating intellectually. And because there are so many open jobs to fill, this sector is also attractive financially. But joining the cybersecurity industry also means having a significant impact on society. We live in a digital world where protecting data and individual privacy has become a critical sustainability issue. And as always, women play a vital role in making this possible. \$\mathbb{1}\$

SECURING WORKLOAD COMMUNICATION

IHAB FARHOUD, SOLUTION ENGINEERING DIRECTOR — MIDDLE EAST, TURKEY, AND NORTH AFRICA, VMWARE TELLS ANITA JOSEPH WHY SECURE WORKLOAD ACCESS IS IMPORTANT IN TODAY'S COMPLEX THREAT LANDSCAPE



ow serious is the ransomware threat today? How complex has it become?

Ransomware presents a

Ransomware presents a serious threat to all organisations, but especially those with sensitive information, and continues to grow in complexity. Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. It challenges organisations' information security practices at a very fundamental level, as attackers use everything from social engineering to brute-force attacks and vulnerability exploits to gain entry into corporate networks.

Ransomware attacks exploit all gaps in an organisation's security. Defending against these attacks involves a mix of approaches, from a return to information security basics, inclusion of new technology and defense tactics, and organisational procedural changes. In many ways the process changes are the hardest because they are cultural changes, and cultural change is the hardest type of change to make. The "if it ain't broke don't fix it" mentality is still pervasive in most organisations, and proactive change under

that attitude is hard, at least until a very public breach occurs.

To become resilient to ransomware means that an organisation needs to address it at many different levels, and through technical and non-technical means.

With multi-cloud environments becoming popular, how can companies ensure security of their systems and data?

Most organisations should consider a Zero Trust program, but this holds especially true for those that are experiencing significant changes through cloud migrations/transformations and application modernisations.

As rapid cloud adoption is met with new models of computing that support rapid application development, the rise in cloud-native applications, and workload-focused ransomware attacks, require that organisations look one step further.

VMware can help with extending Zero Trust for secure workload access. Secure workload access describes the security controls that enable secure communication between workloads and applications both inside and between public and private clouds. It applies Zero Trust principles to enterprise application workloads and data.

Secure workload access addresses the following:

East-west cloud controls. Zero Trust advocates for perimeter-less security, meaning that it must be infused into the network and inside the public or private cloud. VMware can ensure that workloads are segmented within the network to prevent lateral movement of attackers and network exploitation. Workload communication can be secured and inspected with signature- and behavior-based techniques to detect threats. Finally, VMware's Service Mesh can protect access to APIs exposed by modern application workloads.

Cloud-to-cloud edge controls. Edge controls help protect your enterprise closer to where business happens. These controls include firewalls with advanced threat protection and secure cloud-to-

cloud connectivity. They also include web applications and API security to protect your individual applications from incoming threats.

For these controls to be operationalised at scale, they need to be elastic, distributed, workload-attached given the dynamic environment within the cloud, and have automated policy support.

Why is threat detection important and how can organisations go about prioritising this?

Cyber attackers are continuously developing ever-more sophisticated strategies to gain access to networks. These attacks are typically well-funded, often specifically targeted, and involve complex malware that is designed to avoid common security defenses. Countering advanced threats requires advanced analytic tools that can provide rapid visibility, analysis, context, and response into the contents and actions of malicious network traffic.

Threat detection is a key component of Advanced Threat Protection (ATP), a suite of analysis tools designed to defend against advanced threats that use known and unknown attack vectors. ATP augments more common security solutions aimed at repelling known intrusion strategies.

MOST ORGANISATIONS
SHOULD CONSIDER
A ZERO TRUST
PROGRAM, BUT THIS
HOLDS ESPECIALLY
TRUE FOR THOSE THAT
ARE EXPERIENCING
SIGNIFICANT
CHANGES THROUGH
CLOUD MIGRATIONS/
TRANSFORMATIONS
AND APPLICATION
MODERNISATIONS.

Advanced threat protection solutions perform sophisticated detection and analysis on suspicious network traffic, often employing hardware emulation and supervised and unsupervised machine learning models. ATP solutions attempt to identify threats early – before they can do damage – and respond quickly in the event of a breach. The goal is to protect the network with the highest possible fidelity insights into the most challenging threats.

What's the threat landscape looking like in 2022?

The threat landscape is evolving rapidly and organisations and individuals must exert caution. To highlight just few anticipated trends: If 2021 was the year of the Zero Day, 2022 will be the year of Zero Trust. As Eric O'Neill, National Security Strategist at VMware, stated recently, "In 2021, defenders caught the highest number of Zero Days ever recorded. We saw a massive proliferation of hacking tools, vulnerabilities, and attack capabilities on the Dark Web. As a response, 2022 will be the year of Zero Trust where organisations 'verify everything' vs. trusting it's safe. Governments and organisations will adopt a Zero Trust mindset with the assumption that they will eventually be breached. A Zero Trust approach will be a key element to fending off attacks in 2022."

We also look set to see adversaries move laterally and exfiltrate data from unsecure multi-cloud environments. As Chad Skipper, Global Security Technologist, VMware, said recently: "With multi-cloud environments on the rise, the attack surface will continue to expand. This will invite greater proliferation of common ports and protocols that will be used by the adversary to move laterally and exfiltrate data once inside an organisation's network. In 2022, we will see the adversary focus their efforts on living and hiding within the common noise of an organisation's networks. Having visibility into this noise to identify the adversary will become more essential than ever before when defending today's multi-cloud environments." 🙎

GARTNER IDENTIFIES TOP SECURITY AND RISK MANAGEMENT TRENDS FOR 2022

SECURITY LEADERS MUST EVOLVE STRATEGIES TO PROTECT AN EXPANDING DIGITAL FOOTPRINT AGAINST EMERGING THREATS

ecurity and risk management leaders must address seven top trends to protect the ever-expanding digital footprint of modern organisations against new and emerging threats in 2022 and beyond, according to Gartner, Inc.

"Organisations worldwide are facing sophisticated ransomware, attacks on the digital supply chain and deeply embedded vulnerabilities," said Peter Firstbrook, research vice president at Gartner. "The pandemic accelerated hybrid work and the shift to the cloud, challenging CISOs to secure an increasingly distributed enterprise – all while dealing with a shortage of skilled security staff."

These challenges lend themselves to three overarching trends impacting cybersecurity practices: (ii) new responses to sophisticated threats, (ii) the evolution and reframing of the security practice and (iii) rethinking technology. The following trends will have broad industry impact across those three domains:

Trend 1: Attack Surface Expansion

Enterprise attack surfaces are expanding. Risks associated with the use of cyber-physical systems and IoT, open-source code, cloud applications, complex digital supply chains, social media and more have brought organisations' exposed surfaces outside of a set of controllable assets. Organisations must look beyond traditional approaches to security monitoring, detection and response to manage a wider set of security exposures.

Digital risk protection services (DRPS), external attack surface management

ORGANISATIONS
MUST LOOK BEYOND
TRADITIONAL
APPROACHES TO
SECURITY MONITORING,
DETECTION AND
RESPONSE TO MANAGE
A WIDER SET OF
SECURITY EXPOSURES.

(EASM) technologies and cyber asset attack surface management (CAASM) will support CISOs in visualising internal and external business systems, automating the discovery of security coverage gaps.

Trend 2: Digital Supply Chain Risk

Cybercriminals have discovered that attacks on the digital supply chain can provide a high return on investment.

As vulnerabilities such as Log4j spread through the supply chain, more threats are expected to emerge. In fact,

Gartner predicts that by 2025, 45% of organisations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.

Digital supply chain risks demand new mitigation approaches that involve more deliberate risk-based vendor/partner segmentation and scoring, requests for evidence of security controls and secure best practices, a shift to resilience-based thinking and efforts to get ahead of forthcoming regulations.



Trend 3: Identity Threat Detection and Response

Sophisticated threat actors are actively targeting identity and access management (IAM) infrastructure, and credential misuse is now a primary attack vector. Gartner introduced the term "identity threat detection and response" (ITDR) to describe the collection of tools and best practices to defend identity systems.

"Organisations have spent considerable effort improving IAM capabilities, but much of it has been focused on technology to improve user authentication, which actually increases the attack surface for a foundational part of the cybersecurity infrastructure," said Firstbrook. "ITDR tools can help protect identity systems, detect when they are compromised and enable efficient remediation."

Trend 4: Distributing Decisions

Enterprise cybersecurity needs and expectations are maturing, and executives require more agile security amidst an expanding attack surface.

Thus, the scope, scale and complexity of digital business makes it necessary to distribute cybersecurity decisions, responsibility, and accountability across the organisation units and away from a centralized function.

"The CISO role has moved from a technical subject matter expert to that of an executive risk manager," said Firstbrook. "By 2025, a single, centralized cybersecurity function will not be agile enough to meet the needs of digital organisations. CISOs must reconceptualize their responsibility matrix to empower Boards of Directors, CEOs and other business leaders to make their own informed risk decisions."

Trend 5: Beyond Awareness

Human error continues to be a factor in many data breaches, demonstrating that traditional approaches to security awareness training are ineffective.

Progressive organizations are investing in holistic security behavior and culture programs (SBCPs), rather than outdated

compliance-centric security awareness campaigns. An SBCP focuses on fostering new ways of thinking and embedding new behavior with the intent to provoke more secure ways of working across the organisation.

Trend 6: Vendor Consolidation

Security technology convergence is accelerating, driven by the need to reduce complexity, reduce administration overhead and increase effectiveness. New platform approaches such as extended detection and response (XDR), security service edge (SSE) and cloud native application protection platforms (CNAPP) are accelerating the benefits of converged solutions.

For example, Gartner predicts that by 2024, 30% of enterprises will adopt cloud-delivered secure web gateway (SWG), cloud access security broker (CASB), zero trust network access (ZTNA) and branch office firewall as a service (FWaaS) capabilities from the same vendor. Consolidation of security functions will lower total cost of ownership and improve operational efficiency in the long term, leading to better overall security.

Trend 7: Cybersecurity Mesh

The security product consolidation trend is driving integration of security architecture components. However, there is still a need to define consistent security policies, enable workflows and exchange data between consolidated solutions. A cybersecurity mesh architecture [CSMA] helps provide a common, integrated security structure and posture to secure all assets, whether they're on-premises, in data centers or in the cloud.

"Gartner's top cybersecurity trends don't exist in isolation; they build on and reinforce one another," said Firstbrook. "Taken together, they will help CISOs evolve their roles to meet future security and risk management challenges and continue elevating their standing within their organisations."

THE VISIBILITY FACTOR

RAM VAIDYANATHAN, PRODUCT MANAGER AT MANAGEENGINE, TELLS ANITA JOSEPH WHY CASB IS A KEY TOOL IN PREVENTING DATA LEAK AND PROVIDING MORE VISIBILITY FOR SHADOW APPLICATIONS.



a while, but it's becoming the buzzword now. Tell us more about it. Think of cloud access security broker (CASB) as a midpoint between the end users of an organisation and the cloud applications that they're trying to access. Nowadays, with all data moving to the cloud and people opting to work from wherever they please, it makes sense to have a CASB in the middle to help with two main things, the first of which is data leak prevention. So, any time any sort of data is uploaded onto the cloud from an organisation, it can get that visibility for you. At the same time, it can give visibility about shadow applications. Let

ASB has been around for

There are two main kinds of applications: blacklisted and whitelisted. Blacklisted refers to applications that are clearly banned by the organisation, and whitelisted refer to applications sanctioned/

me explain this better.

permitted by the organisation to be used by employees. Then there is a third category called shadow applications which the IT team of an organisation has no idea about. These applications are neither banned, nor are they sanctioned, so there needs to be a policy put in place for these applications. CASB will give visibility about these shadow applications. It will list out for the IT teams all the shadow applications that different users have requested and the IT teams can then take policy decisions on whether to sanction or ban these shadow applications.

How is ManageEngine positioning itself in this fast growing, extremely volatile threat-attack landscape today?

With ManageEngine, what we would like to give customers are unified solutions that help investigate, detect and respond to threats. We want to provide a 360-degree view of all activities that happen in a company's network, all on one single console. Incidentally, CASB is also a critical component that adds security context for our customers and it can be used in tandem with all the other components as well. With all this visibility comes higher fidelity when it comes to threat detection in an extremely volatile landscape.

In your opinion, what are some of the top security trends for 2022, particularly the region?

With remote/hybrid working becoming the new normal, organisations now need to cater to multiple environments. This means that organisations use the public cloud, the private cloud, then there's the on-premises environment as well. The data is spread across these different environments. This becomes

a huge security challenge. How should organisations get visibility across these platforms where data may be dispersed?

Secondly, when it comes to the cloud, organisations are going with multiple cloud vendors. Organisations could deploy AWS, Azure, Salesforce, Alibaba Cloud, and more. Getting visibility and being able to monitor all the activities that happen in a multicloud environment is another security challenge.

Ransomware is yet another challenge during the present times. Today's ransomware attacks not only encrypt files but also steal data and threaten to release them publicly if the ransom is not paid. Thus, it has morphed into double extortion ransomware. We will also see more cases of distortionware, wherein attackers target the operational technology of an organisation apart from the IT.

What is ManageEngine's plan for 2022 in the SIEM space?

In 2022, there are primarily three

"WITH
MANAGEENGINE,
WHAT WE WOULD
LIKE TO GIVE
CUSTOMERS
ARE UNIFIED
SOLUTIONS THAT
HELP INVESTIGATE,
DETECT AND
RESPOND TO
THREATS."

things that we would like to do. One is that in addition to our SIEM capabilities, we also want to focus on SOAR, a term defined by analysts referring to Security Orchestration, Automation and Response. ManageEngine Log360 is an integrated SIEM and SOAR solution. We want to enhance our capabilities when it comes to SOAR. This is something that we are very diligently working on. We want to bring in more automations and integrations with third parties so that we can ramp up our incident response features. So it is not just about attack detection or threat detection, we also want to enhance our response and mitigation capabilities.

The second thing that that we would like to do in 2022 is work on enhancing our CASB capabilities. There's a whole lot more that we can achieve with CASB. Right now, we are doing CASB through the forward proxy method, but there are other ways of accomplishing that, which can also help solve more security use cases. So, we would like to get into that sphere also and this is something that we have in our roadmap.

The third thing I would say is having more security- related use cases which are going to be built out-of-the box within Log 360. We are a vendor who constantly studies the market and talk with our customers. We want to build more of these security use cases for the 2022 threatscape.

Here, I'd like to point out that ManageEngine Log360 is a Unified SIEM solution. It has also got CASB capabilities now, as well as data leak prevention capabilities. As we further enhance our product, we would like to work with more and more SMBs and enterprises alike. 1

NOZOMI NETWORKS LABS REPORT: RANSOMWARE GANGS AND SUPPLY CHAIN VULNERABILITIES **HIGHLIGHT RISKS AS LAW ENFORCEMENT FIGHTS BACK**

WHILE VULNERABILITY DISCLOSURES INCREASED 21% IN THE SECOND HALE OF 2021 AND INCREASINGLY SOPHISTICATED CRIMINAL ATTACKS MADE REGULAR NEWS ORGANISATIONS ARE FIGHTING BACK WITH TARGETED REMEDIATION FEFORTS



their ability to disrupt society. More than 651 vulnerabilities were reported from July through December—a 21-percent increase over the previous six months. Supply chain vulnerabilities continue to offer the greatest opportunity to quickly spread damage across a wide range of products, service providers or end users.

For the first time since Nozomi Networks began publishing the bi-annual report, there are early signs that defenders are maturing their strategies for security and resilience and may be starting to gain

an upper hand. In the second half of the year, international law enforcement agencies combined efforts to take down ransomware gangs, seize bitcoin bounties and make criminal

arrests. And, in spite of predictions that the Apache Log4j vulnerability would be the most widely exploited security breach ever, the attacks have not seen the catastrophic loss that was predicted.

"Security organisations and law enforcement are punching back," said Nozomi Networks Co-founder and CTO Moreno Carullo. "We are seeing some good signs that more security professionals are modernising their defenses to address both prevention and resiliency, and that a post-breach

FOR THE FIRST TIME SINCE NOZOMI **NETWORKS BEGAN PUBLISHING THE BI-**ANNUAL REPORT. THERE ARE EARLY SIGNS THAT DEFENDERS **ARE MATURING** THEIR STRATEGIES **FOR SECURITY AND RESILIENCE AND MAY BE** STARTING TO GAIN AN **UPPER HAND.**

mindset is paying off. Threats may be on the rise, but technologies and practices to defeat them are available now as we have greater insights into the nature of the vulnerabilities and attacks. We encourage more organisations to strengthen their security and situational awareness so they too are prepared in the face of an attack."

Nozomi Networks' "OT/IoT Security Report" provides security professionals with the latest insights needed to re-evaluate risk models and security initiatives, along with actionable recommendations for securing critical infrastructure. 1

new OT/IoT security trends report from Nozomi Networks Labs finds that while ransomware and Ransomware as a Service (RaaS) attacks continued to dominate cybercriminal activity in the second half of 2021, there was a slight uptick in statesponsored actions as global tensions rise.

Critical infrastructure such as healthcare, transportation and food production are increasingly seen as highly vulnerable and lucrative targets based on

SAMSUNG

Smart Monitors The World's 1st Do-it-All Screen.

M5 Series Full HD: 24 27 32





M7 Series 4K UHD with USB-C: 32 43





DESIGN AWARD 2021







prime video



NETFLIX











Partnership Beyond Business Authorized Distributors



TAKE THE GUESSWORK OUT OF CRITICAL INFRASTRUCTURE CYBERSECURITY

SAKET MODI, CO-FOUNDER AND CEO AT SAFE SECURITY

he disruption of critical infrastructure has a ripple effect on national and global economies and societies; directly impacting the sovereignty of nations and its people. When a Colonial Pipelines, Wolf Creek Nuclear Operating Corporation, or a Springhill Medical Center cyberattack happens repeatedly across the world, the entire critical infrastructure security ecosystem needs to be re-imagined.

A modern-day cyberattack leverages vulnerabilities across the spectrum. Starting from employee social media reconnaissance, purchasing ransomware toolkits off the deep and dark web, leveraging cloud misconfigurations to move laterally within connected systems and networks, and targeting their efforts to compromise the most vulnerable vendors - cybercriminals are maximizing impact with minimum effort.

When cyberattacks are so interconnected, then why is the cybersecurity of critical infrastructure siloed and reactive?

The convergence of IT and OT has revealed more vulnerabilities in Critical Infrastructure.

In previous years, cyberattacks on critical infrastructure typically required high investments, physical reconnaissance, and access to expensive operational technology. The isolated nature of this sector, yielding low output, ensured threat actors focused their energies on more 'rewarding' fields, often including financial services or healthcare.

As business demands for speed, efficiency, and interoperability increased, the critical infrastructure sector adapted. Most critical systems were extremely complex, to begin with, and this complexity is only increasing as the

number of IoT devices and connections grows. Additionally, these systems are a mix of unsecured legacy systems and modern technology. The convergence of Information Technology and Operation Technology systems in the critical infrastructure setup have made it a hotbed of cyber threats.

Especially in the Middle East that is at the forefront of 5G and loT implementation, the pandemic added velocity to a change that was in motion. Transitioning to cloud-based technologies has created a 'Swiss Cheese' architecture with multiple entry points - employees are geographically dispersed, connecting to workloads and data that's now in a multi-cloud fabric. Additionally, customers and suppliers have changed the way they function. The number one issue with a vast digital footprint is the lack of real-time security visibility. Without the right knowledge of



cyber risk, businesses are basing their cybersecurity strategies on reactive threat-driven strategies. This is similar to driving forward on a busy highway, while only looking at the rearview mirror!

Businesses need a totalistic and contextual view of their cyber risk posture, and move beyond a product-focused approach and reactive cybersecurity. This

is where cyber risk quantification (CRQ) can be a game-changer.

Cybersecurity is all about knowledge

Cyber Risk Quantification platforms enable security leaders to take the guesswork out of cybersecurity by giving them sound data science-driven basis to measure, manage, and mitigate cyber risks. When a business knows the risks involved, they're able to make informed decisions about their cybersecurity initiatives.

Cyber Risk Quantification platforms generate a breach-likelihood score using data science-backed risk engines that can feed information-driven confidence to security teams. It aggregates signals across employees, technology, policies and processes, cybersecurity products, and third (nth) parties to generate a score. With it, security teams can locate where the weakest links lie across the enterprise in real-time. Not only does this help in timely prioritising management and mitigation of cyber risks, but also informs the Board and other stakeholders about the efficiency of their cybersecurity strategy, products in use, and return on investment. How? Risk Quantification can represent the likelihood of breach as the financial impact of a breach on the overall business - immediately putting cyber risk in perspective to all relevant stakeholders.

Cybersecurity is like a game of chess, where the one with the knowledge and predictive power of the next move has the advantage. To date, cybercriminals have been one step ahead. To succeed, the national and international cybersecurity strategy for critical infrastructure protection (CIP) needs to be predictive and simplified. Cyber risk quantification can provide governments and businesses with the proactive knowledge to make the right move.

The tactics, techniques, and procedures used by the new-age cybercriminal use the 'compromise-one-compromise-many' approach. As the lines between private and public blur in critical infrastructure, it is essential to proactively safeguard the information of citizens, ensure smooth functioning of all associated organisations, and finally, prevent large-scale disruption. \$\mathbb{1}\$

SECURING THE APP LANDSCAPE

MOHAMMED ABUKHATER, VICE-PRESIDENT, MIDDLE EAST, TURKEY & AFRICA AT F5 TELLS ANITA JOSEPH WHY APPLICATION SECURITY IS KEY TO A ROBUST DEFENCE AGAINST ATTACKS



hy is application security important today? Cybercriminals are motivated by money, and they use their time on the activities that have the highest return. In a digital economy, attackers target applications and APIs to exploit vulnerabilities and abuse business logic, compromising customer accounts and committing large-scale fraud that can devastate business operations.

Application security is vital because apps are ubiquitous and form the backbone of most modern digital services. If applications fail, due to security or any other reason, it disrupts customers' experience and causes both short-term and long-term damage to the organisation and their brand. In a worstcase scenario, it can cause a business to become untenable.

A major challenge businesses face is that when they try to thwart cyberattackers, they also inadvertently frustrate legitimate users, and this can lead to abandoned transactions and lost revenues. Worse still, many of the conventional tools that organisations use to try to prevent cyberattacks are easily bypassed by motivated cybercriminals.

In this light, application security must protect strategic business outcomes

including revenue and customer growth.

That is why F5 application security solutions protect apps and APIs across architectures, clouds, and ecosystem integrations to reduce risk and operational complexity while accelerating digital transformation. By doing so, you can improve time to market, maximise business potential, and maintain resilience to ensure consistent delivery of secure digital experiences at scale.

What are some of the critical risks that applications are facing today?

Cybercriminals use large groups of bots to automate vulnerability exploits and accelerate commercial fraud. Furthermore, readily available compromised data and tools provide attackers with an attractive ROI, and the risk surface is growing as modern apps are decentralised and more data moves to the edge. Strategic business initiatives such as revenue generation, customer loyalty and brand-building leverage APIs and third-party integrations, which can create blind spots that can be hijacked resulting in data breaches, account takeovers and fraud. Customers demand trusted digital experiences, but apps are complex, which makes it more challenging to secure them.

What are some of F5's products & solutions that help organisations address application security?

F5 recently announced a major expansion of its application security and delivery portfolio with F5 Distributed Cloud Services, which provide security, multi-cloud networking, and edge-based computing solutions on a unified software-as-a-service (SaaS) platform. The company is also launching the first new solution on this platform, F5 Distributed Cloud WAAP (Web Application and API Protection), which augments multiple security capabilities across F5 technologies in one SaaS offering.

F5 Distributed Cloud WAAP simplifies security and automates processes for

CUSTOMERS DEMAND TRUSTED DIGITAL EXPERIENCES, BUT APPS ARE COMPLEX, WHICH MAKES IT MORE CHALLENGING TO SECURE THEM.

organisations across all industries, allowing application teams to focus on delivering features and functionality that will enhance their customers' experience and propel their businesses forward. The new SaaS-based offering integrates F5's industry-leading web application firewall, bot mitigation, DDoS, and API protection capabilities into a single, easy-to-deploy solution that enables SecOps and DevOps teams to enforce consistent security policy wherever they need to deploy applications.

What is the application security landscape looking like in 2022?

In F5's upcoming 2022 State of Application Strategy Report, 88 percent of organisations say they operate both legacy and modern application architectures, while 70 percent operate in multiple clouds. This expands the threat surface area as companies are forced to deploy separate, and often inconsistent, security controls across different environments. Add to this the changing threat landscape (see below), and you can see why it is imperative for organisations to invest in effective application security.

2022 will be an eye-catching year for cybersecurity incidents, fallouts, and innovations. F5 Labs recently made predictions for the year ahead, including the following:

1. State-sponsored actors will adopt cybercrime toolsets

This year, we expect to see more advanced persistent threats (APTs),

specifically state-sponsored actors, modifying known commodity malware strains and using techniques cybercriminals have become famous for, such as setting up command-and-control (C&C) over Telegram messenger.

2. Fintechs will front for collecting credentials

While many fintechs are well established and reputable, others come and go. My prediction? In 2022, we will learn that one or more fintechs were nothing more than a front for a criminal organisation established only to collect usernames and passwords.

3. The cloud will eat traditional IT

We're nearing a tipping point where the cloud will become a part of default IT skills. With multi-cloud becoming the new normal, there will be growing expectations that IT pros have the requisite skills.

4. Ransomware will target the rich

It is only a matter of time before somebody starts targeting the extremely wealthy on their own personal networks. These targets clearly have the means to pay the ransom, and their information systems are often as complex as those of small enterprises.

5.Organisations will have more key problems

You can secure private keys by encrypting the key file and using a passphrase, but as the number of keys you manage increases, this can quickly get out of hand—you can easily end up with a duplicate password scenario. For enterprises and large organisations, cloud HSM services should look like the only way to go, but I think that it even makes sense for individual power users. However, it's just a question of whose keys get compromised this year. So, get yourself a secure key storage tool and make sure you're not one of the compromised. 1



معرض و مؤتمر الخليج العالمي لأمن المعلومات



GLOBAL

21 - 23 MARCH 2022 | DUBAI WORLD TRADE CENTRE

ARAB WORLD'S UNRIVALLED

CYBERSECURITY BUSINESS EVENT

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

> H.E. Dr. Mohamed Al-Kuwaiti, Head of Cyber Security, United Arab Emirates Government

ENQUIRE ABOUT EXHIBITING, SPEAKING AND SPONSORSHIP

971 (04) 308 6267 | gisec@dwtc.com | #GISEC

OFFICIALLY SUPPORTED BY

OFFICIAL GOVERNMENT CYBERSECURITY PARTNER OFFICIALLY SUPPORTED BY











هيئة تنظيم الاتصالات والحكومة الرقمي

OFFICIAL DISTRIBUTION PARTNER







ORGANISED BY







ISSUE 63 | MARCH 2022 WWW.TAHAWULTECH.COM

SECUI RIDDLE EAST







he cybersecurity landscape today is a dynamic, evolving, multifaceted one. Particularly post the pandemic, attacks have become more frequent and the approaches more targeted, and so the battle between the attackers and defenders is on in full swing. APT attacks, ransomware, phishing-these have been plaguing the region for a while now and according to reports, the attacks are only set to become more worrisome and unpredictable. The main focus of organisations in the region is to diversify their defence strategies and create more awareness among their employees about the need to remain vigilant and alert about cyber vulnerabilities and data protection.

To those keenly watching this space, there is no better opportunity to get more perspective than GISEC-the most awaited event of the year-providing the ultimate opportunity to experience the full-powered synergies of cyber security across industries, across enterprises and across governments.

GISEC is the undisputed show for security business and the industry's leading super-connector – bringing together global cybersecurity providers and powerhouse vendors from all over the world, globally renowned hackers, heads of national security agencies and CISOs of major corporations. For three days, the World Trade Centre in Dubai will witness scintillating discussions, robust brainstorming sessions, a healthy exchange of ideas and best practices, as the who's who of cybersecurity in the region debate the best cyber defence strategies and

approaches to tackle the complex and complicated threat-attack landscape. Innovation will be the buzzword here as decision-makers come together to debate a comprehensive defence strategy to tackle the growing threats.

With numerous national pavilions set to showcase best-in-class solutions from a host of the globe's major cybersecurity solution providers. GISEC 2022 will deep-dive into the most pressing cybersecurity challenges affecting enterprises and governments in the post-pandemic era. The latest edition of GISEC will focus on ethical hacking through a number of interactive onsite features and activations taking place throughout the three days. One of the highlight activations comes in the form of the largest live Bug Bounty hunt ever to take place in the UAE.

In support of the UAE Cyber Security Council National Bug Bounty Program, 100 ethical hackers are flying in to take part in the GISEC Bug Bounty programme, where they will be tasked

INNOVATION
WILL BE THE
BUZZWORD HERE AS
DECISION-MAKERS
COME TOGETHER
TO DEBATE A
COMPREHENSIVE
DEFENCE STRATEGY
TO TACKLE THE
GROWING THREATS.

to hack, identify, and fix certain software flaws in a number of different scenarios and mainframes – including electric cars, mobile phones and drones.

GISEC is also set to host the biggest, most comprehensive cybersecurity platform in the region, with an expanded conference line-up that is set to feature more than 200 highcalibre speakers, including national cybersecurity leaders, tech pioneers, policymakers, researchers and intelligence heads. The UAE Cyber Security Council will host the Global Cybersecurity Congress – an annual gathering aimed at unifying efforts on local, national and global cross-sector levels and shaping national security and defence strategies to combat evolving threats; and a multitude of training workshops for industry professionals.

GISEC 2022 builds on its decades of relationships with the global InfoSec community, corporate leaders, endusers from government and major buyers of cybersecurity solutions. With the MEA cybersecurity market expected to reach \$2.89 billion by 2026 at a CAGR of 7.92% over the next four years, according to Mordon Intelligence, GISEC 2022 will see the world's leading cybersecurity providers showcase their latest products, solutions, innovations in the fields of cloud security, ransomware exploring collaborative business opportunities at the event.

In this special section we present some of the security frontrunners who are redefining the cybersecurity space with their pro-active approach, comprehensive strategies and targeted responses.

SECURING CYBERSPACE



lease tell us about the products and solutions you are showcasing at the event and how can CISOs benefit from these?

During GISEC, ESET will present its APT solutions that are witnessing rapid adoption across organisations of all business sizes and industry segments. ESET will showcase ESET Inspect, the XDR-enabling component of the ESET PROTECT platform helping enterprises protect against advanced persistent threats, and secures them from zero-day threats and highly targeted malicious attacks. The solution bundle offers granular visibility, risk assessment, incident response, investigation and remediation helping IT Security Professionals to strengthen the cybersecurity posture of the organisation.

By the way, ESET solutions has earned a distinction in 2022 for being named as the 'Top Player' in the Radicati Advanced Persistent Threat Market Quadrant for the third time in a row, leading ESET achieve the best position among all the European-based security vendors.

What are some of the threats that organisations must watch out for, in 2022? How is your company approaching these threats?

Ransomware is still the prime threat that is growing aggressively and surpassed the worst expectations in 2021, with attacks against critical infrastructure, outrageous ransom

WHEN SELECTING THE RIGHT MFA SOLUTION, BEARING SECURITY STANDARDS IN MIND IS A WAY OF ENSURING THAT YOUR SOLUTION IS ENTERPRISE-READY, FUTURE-PROOFED AND WILL INTEGRATE EASILY INTO YOUR EXISTING IT INFRASTRUCTURE."

demands and over USD 5 billion worth of bitcoin transactions tied to potential ransomware payments identified in the first half of 2021 alone.

Remote Desktop Protocol (RDP) attacks are on the rise. The numbers from the last weeks of ESET T3 2021 Threat Report broke all previous records, amounting to a staggering yearly growth of 897% in total attack attempts blocked.

Malware attacks does not seem to slow down anytime soon and will remain cause of major concern in 2022. Last year, ESET noted an alarming upsurge in Android banking malware detections, which rose by 428% in 2021 compared to 2020.

What are some of the leading cybersecurity approaches/ postures that are gaining traction this year?

It is of the paramount importance to ensure organizations have effective digital security solutions in place, but it is also critical to note that these solutions are only one component of a good cybersecurity posture.



There are a few approaches organizations can take to enhance their defenses, which includes the following

- Stay up-to-date with the latest threat landscape and review security posture regularly with a trusted cybersecurity advisor
- Consider endpoint detection & response (EDR) to enhance never-before-seen threat detection capabilities and response
- Implement a zero-trust security model to mitigate any security risks.
- Implement Multi-factor Authentication (MFA) to prevent password

breaches & Data Leakage Prevention (DLP) to avoid any sensitive data from leaking outside the corporate network.

- Improve employees' cyber hygiene by providing regular cybersecurity awareness training
- Ensure best practices are in place and processes are supported by the right technology

Tell us about your company's range of products and solutions and what's the best defence they offer against today's threat/attack scenario?

Backed by a strong R&D, today ESET

boosts one of the most robust portfolio of digital security solutions in the world that are ratified and authenticated by the leading independent organisations worldwide. Our portfolio includes both consumer and business digital security solutions that helps individuals, startups, small businesses to large enterprises protect themselves against the latest threats. Each single product or solutions from our portfolio addresses the specific concern and provides the best possible defence a digital security solution can provide in the world. \$\mathbb{1}\$

IMPORTANCE OF MULTIFACTOR AUTHENTICATION (MFA) OVERVIEW

ANDREW BULL, IDENTITY & ACCESS MANAGEMENT SOLUTIONS. SR. DIRECTOR, STRATEGIC SALES AT HID GLOBAL

s our organisations and the IT infrastructures we use are continually evolving, the ways in which they can become vulnerable are equally changing. In recent times, the occurrence of security breaches and the levels of sophistication they have reached is an increasing worry for modern day organisations. Large scale attacks such as the SolarWinds Orion software breach and well publicised Microsoft Exchange hack are a serious warning to the importance of having a strong cybersecurity strategy - no matter how big or small an organisation.

In the light of increasing security threats and pressure for organisations to deploy strong MFA, many security professionals are now considering MFA on a wide-scale basis across their organisations. MFA is not 'one size fits all' - there are numerous factors to consider such as enhance security, boost user experience, but also deploy a solution that is versatile enough to address your organisation's unique use cases, workflows, and security needsboth now and in the future.

The answer is choosing a vendor that

is a 'one-stop shop' for every part of the MFA journey. With the market's leading solution for managed authentication credentials and support for multiple security standards, authentication methods and form factors, deploying a complete and versatile MFA ecosystem is made easy with HID.

Tailoring an MFA solution to solve your unique use cases

Your users need to access countless resources throughout their working day, which means there's a whole host of

WHEN SELECTING THE RIGHT MFA SOLUTION, BEARING SECURITY STANDARDS IN MIND IS A WAY OF ENSURING THAT YOUR SOLUTION IS ENTERPRISE-READY, FUTURE-PROOFED AND WILL INTEGRATE EASILY INTO YOUR EXISTING IT INFRASTRUCTURE."

places where MFA could and should be incorporated. Let's explore them all:

Personal Computers- considering the sharp rise of remote workers, providing quick and secure access to personal computers and devices is of high importance. With HID's Crescendo range of authenticators, users can instantly log on to computers by inserting or tapping the smart card or security key to their device.

Shared Workstations- Using workstations that are shared between multiple people poses greater threats for security compromises and is especially important in industries such as healthcare, retail and manufacturing. With HID's award-winning, on-premise MFA solution, DigitalPersona, users can effortlessly move between workstations, with a wide choice of authentication methods ranging from fingerprint and facial through to access cards and PKI credentials.

IT Applications and systems- HID's versatile MFA solution protects everything from VPN, data and cloud applications, such as G Suite, DropBox and Microsoft 365, all the way to legacy desktop applications – so that no resource goes unprotected.

Data Encryption and Digital
Signatures- Here is where your MFA
solution can start to do more than simply
securing a login. By using HID's cloudbased credential management solution,
you can centrally issue and manage PKI
certificates on Crescendo and third-party
credentials – giving you the opportunity to
also digitally sign and encrypt emails and
documents.

Buildings- HID's MFA solution portfolio is unique in that it offers high assurance credentials that can secure access to physical spaces, in addition to digital resources. By incorporating employee badges for converged physical and logical access, you can enjoy the cost efficiency, ease of use and the benefits of streamlining multiple authenticators across your organisation.

Why are security standards and certifications important?

When selecting the right MFA solution, bearing security standards in mind is a way of ensuring that your solution is enterprise-ready, future-proofed and will integrate easily into your existing IT infrastructure. Deploying HID authenticators in your organisation means you can stay compliant with industry recognised standards, including:

- PSD2, PCI-DSS, GLBA, NYDFS 23 NYCRR 500 for payments and financial institutions
- CJIS, IRS pub 1075 for law enforcement organizations
 - NERC-CIP for critical infrastructure
 - HIPAA for healthcare organisations
- NIST SP800-171, SOX for enterprise and non-federal organisations.

MFA Is Not Only for Governments and the Private Sector Should Follow Their Lead.

Beyond the Government, other Key Verticals include Healthcare, Financial Services, Manufacturing, Education and Retail. With MFA solutions like DigitalPersona, organisations can layer the authentication requirements to meet specific use cases and step up when needed and can incorporate a wide selection of devices and authentication methods: Biometrics, Multi-protocol smart cards, such as HID Crescendo (FIDO, PKI, PIV, OATH, and physical access capabilities for converged physical and logical access), Security keys, such as HID Crescendo Key Series with support for NFC, USB-A and USB-C, Building access cards, One-time password tokens, Bluetooth and NFC devices, mobile push authentication, and more.

DigitalPersona

A key element within HID Global's multi-factor authentication portfolio, HID DigitalPersona® transforms the way IT professionals protect the integrity of their digital organisation by going beyond traditional two factor and multi-factor



authentication. The solution supports various applications, including websites, cloud, Windows, mobile, VDI and VPN and the broadest array of authentication factors which include contactless cards, smart cards, security keys, mobile and OTP tokens, and biometrics including facial recognition, behavior, and fingerprint.

Free trial available.

HID Crescendo

HID Crescendo enables organisations to secure access to valuable corporate resources and meet regulatory compliance with user-friendly, quick-to-deploy and easy-to-manage multi-factor authentication. Thousands of employees across the world use HID's high

assurance credentials for passwordless and phishing-resistant authentication and SSO protection, secure log-in to VPN, servers, Azure Active Directory and any application protected by it, Windows and shared workstations, digital signature and data encryption. Organisations have the flexibility to choose from smart cards or security keys (NFC, USB-A and USB-C) with support for FIDO2, PIV/ PKI, OATH as well as various physical access technologies to form a Zero Trust security infrastructure across their organisation. From managed to stand-alone, it is a versatile solution that supports more use cases than any other solution in the identity and access management market.

Free samples available. 🙎

BARRACUDA TO FOCUS ON ENABLING BUSINESSES SECURE WEB APPS & EMAIL AT GISEC

n line with cybersecurity risks outlined in its latest spearphishing report, Barracuda will participate at GISEC, and focus on the theme 'Securing Applications and Email'. The company, which earlier this year announced its partnership with Finesse, a global system integration company, will participate together with this regional partner and intends to showcase to customers how Finesse's expertise in digital transformation, complemented by the power and simplicity of Barracuda's cybersecurity solutions portfolio, can enable them to reduce cybersecurity risk on their digital journeys.

WE HOPE TO
ACCOMPLISH
IS MEANINGFUL
ENGAGEMENTS
THAT ENABLE US
TO COLLABORATE
WITH A WIDER
NUMBER OF
CUSTOMERS AND
PARTNERS.

Outlining key objectives of his organisation's participation at GISEC 2022, Toni El Inati - RVP Sales, META & CEE, Barracuda Networks said, "We will be collaborating with our new partner Finesse to raise awareness of our partnership through our participation at GISEC. Given that we have new cybersecurity professionals who have recently joined our regional team, we will also utilise the show as an opportunity to introduce them to existing customers and partners. We are eager to engage with all industry stakeholders to get a deeper understanding of the latest market requirements and developments.



In the end, what we hope to accomplish is meaningful engagements that enable us to collaborate with a wider number of customers and partners."

The 7th edition of Barracuda's 'Spear phishing: Top Threats and Trends' report revealed that phishing and Business Email Compromise (BEC) attacks are among the top three social engineering attacks, accounting for 51% and 9% of the 2021 total respectively. To enable GISEC attendees to effectively counter these threats, the company will showcase Barracuda Total Email Protection, a suite of powerful security solutions that offer protection against a wide range of email threats, at the event.

The report also showed that through 2021, cybercriminals compromised approximately 500,000 Microsoft Office 365 accounts. Having recently announced the regional availability of its Cloud-to-Cloud Backup solution from Microsoft's cloud data centres in the UAE, the company will use GISEC as a platform to raise awareness around this solution that delivers a fast search and restore experience for Office 365 data, including Teams, Exchange Online, SharePoint, and OneDrive.

Further research by Barracuda has shown that 72% of organisations have been breached through web applications.

With applications becoming a primary interface between consumers and the businesses they engage with, securing these critical interfaces is paramount. Through its participation at GISEC, Barracuda intends to demonstrate how its Web Application Firewall (WAF) and WAF-as-a-Service offerings help organisations secure their web applications from OWASP Top 10 threats, DDoS, bots, zero-day, and client-side attacks.

Top executives from Barracuda's regional leadership, sales and channel teams will be present at the stand (A-45 Hall No: 6) through the three days of the event.

SANS INSTITUTE TO HIGHLIGHT INTERACTIVE **CYBERSECURITY TRAINING &** WORKFORCE **DEVELOPMENT AT GISEC 2022**

VISITORS CAN ENHANCE THEIR CYBERSECURITY SKILLS AND KNOWLEDGES WITH A RANGE OF ENGAGING ACTIVITIES

ANS Institute, the global leader in cybersecurity training and certifications, has announced their participation at GISEC 2022, to be held at the Dubai World Trade Centre, from March 21 to 23. At GISEC, SANS will showcase a vast range of their offerings, from core training courses, Capture-the-Flag

events (CTFs), security awareness products, knowledge assessments, NetWars tournaments and Cyber Training academies, to educate visitors on how SANS can support organisations in training, recruiting, and retaining cybersecurity staff.

"There is an ever-growing cybersecurity skills gap and need for trained personnel within organisations.

With a growing shortage of people available on the job market, it is becoming increasingly challenging for organisations to find the right talent for the right jobs," said Ned Baltagi, Managing Director, Middle East and Africa at SANS Institute.

"We have many products to offer organisations – small and large – to help them provide their staff with the

WITH A GROWING SHORTAGE OF PEOPLE AVAILABLE ON THE JOB MARKET, IT IS BECOMING INCREASINGLY CHALLENGING FOR ORGANISATIONS TO FIND THE RIGHT TALENT FOR THE RIGHT JOBS.

best possible training experience. As the largest and most anticipated cybersecurity exhibition in the Arab region, GISEC is the best platform to spotlight our larger product portfolio and inform professionals that SANS' proficiencies expand beyond our training courses," Baltagi added.

During GISEC, SANS will offer visitors the opportunity to experience the SANS Secure Middle East 2022 training course, which will take place in Riyadh this month, through their Live Online training format. At stand D21-24, senior executives and cybersecurity experts from SANS Institute will be available to network and share insights on how SANS is working to bridge the current cybersecurity skills gap, as well as how individuals and organisations can adequately protect themselves against the latest cyber threats coming in from nationstate actors. Attendees can also participate in one of the Capture-the-Flag events hosted by

SANS. 1





TECHNOLOGIES APPOINTS ALAIN KALLAS AS SENIOR DIRECTOR, CYBER SERVICES

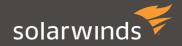
xon Technologies, the
UAE-headquartered
leading information
security solutions provider,
announced the appointment
of Alain Kallas as Senior Director, Cyber
Services. As part of the company's
leadership team, Alain will help expand
Axon's business, and drive sales in the
UAE and globally.

Leading customer engagements and upselling to existing strategic accounts and channel partners, Alain will also work closely with Marie Ange, Axon's Channel and Presales Manager, on key strategic channel accounts. He will help the company identify and win major deals and steer Axon into the next phase of growth and maturity. A key part of his job role also involves engaging with other team leaders inside Axon on how to bridge the gap between sales and delivery.

LEADING CUSTOMER
ENGAGEMENTS
AND UPSELLING TO
EXISTING STRATEGIC
ACCOUNTS AND
CHANNEL PARTNERS,
ALAIN WILL ALSO
WORK CLOSELY
WITH MARIE ANGE,
AXON'S CHANNEL
AND PRESALES
MANAGER, ON KEY
STRATEGIC CHANNEL
ACCOUNTS.

"I have met many cyber experts in my career, and I can honestly say, Alain is up there with the best. His problem-solving approach, deep technical know-how and outstanding client relationships make him a truly complete cyber expert. He has a great skill of combining deep technical experience, with consulting solutions in order to sell clients on the value. We are very excited to have Alain share his learnings and experience with our team and clients," said Hadi Hosn, Chief Executive Officer at Axon Technologies.

Alain brings with him a wealth of experience having spent over 20 years working in cybersecurity. Prior to joining Axon, Alain has held senior roles such as Chief Information Security Officer, Director at Large Cybersecurity Service Providers, Information Security Advisor, amongst others. He has previously worked at SecureWorks, du, and PwC. 1



SECURE BY DESIGN

Leading the Way to Safer IT

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



















Deterministic Protection Platform



Protect full attack surface



Only allows correct execution



Automated runtime protection



Ready-only probe



Zero attacker dwell time



Works with any server

"The world has been far too patient with security vendors who claim to protect against the unyielding ransomware and remote code execution attacks crippling our businesses. Traditional approaches simply do not work. Any CISO or CIO needs to be able to walk into the CEO's office or the boardroom and confidently say that they can not only protect against these attacks but can stop them, within milliseconds, before they do any damage. Virsec is the only company that can give these tech leaders the confidence to say 'Yes!"

- John Chambers,

Former Chairman & CEO, Cisco, and CEO, JC2 Ventures

Recognized Security Leaders

Gartner

CRN



ARN Innovation Awards 2021

MITRE





tahawultech.com CISO50 & Future Security Awards 2021