SPECIAL SUPPLEMENT BY
Enterprise CHANNELS MEA

VOLUME 05 | ISSUE 3 | **MARCH 2023**

CYBER SENTINELS

معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC GLOBAL

SPECIAL

INTEGRATED CYBER SECURITY

Top executives share insights into innovation and integration taking place inside cyber security solutions.

OPX
TECHNOLOGY

FLIPPING TOWARDS INNOVATION

YOUR PARTNER FOR

- Cloud & Digital Transformation
- ERP on Cloud
- Analytics & Automation AI & ML as a Service
- Cyber Security Solutions

Phone: +1 (732) 794-5918 | Email: hello@opxtechnology.com | www.opxtechnology.com

CISOs under pressure

As part of GISEC 2023, GEC Media Group is pleased to bring out its special edition of Cyber Sentinel focussed around innovation in the cyber security industry. Security decision makers face multiple challenges inside their enterprises. These range from increasing attack surfaces and growing complexity to skills shortages and communication with the Board.

So intense is the burnout and pressure on CISOs and CSOs that Gartner recently announced that nearly half of cybersecurity leaders will change jobs by 2025. And from this, 25% will be for different roles entirely due to work-related stress.

Cybersecurity professionals are facing unsustainable levels of stress and are on the defence, seeing only two possible outcomes, to get hacked or not hacked. The psychological impact of this directly affects decision quality and performance of cybersecurity leaders and their teams, was the conclusion made by Gartner analysts.

In the pages ahead, we present how it can be a challenge to secure old systems from modern attacks and a pain to design new systems that do not introduce unnecessary risk. As the regulatory landscape continues to evolve, business leaders must consistently invest in skills and technology to keep updated and stay on the right side of data privacy laws. Organisations must be prepared by admitting that there will be more sophisticated attacks targeting and successfully bypassing multifactor authentication strategies.

To strengthen their security framework, organisations must adopt a holistic security strategy that protects both digital assets and their physical infrastructure and proactively adopt automation and intelligence to improve security. They need to build flexible hybrid infrastructure that can dynamically adapt to changing business requirements.

They also need to establish data-backed policies and controls to prevent bad actors from moving laterally and escalating privileges while setting up analytics-informed policies to assess the changing conditions and adapt access where and when necessary. There is also a need to focus on non-human identities to reduce the risk of privilege-based identity attacks.

CISOs need to keep abreast of international regulations, such as those imposed by SEC, and global best practices while they implement technologies to create a balance in processes for tackling cyberthreats. While businesses must balance their compliance requirements against the need to share data across their digital ecosystems, they also need to plan for the future and design systems that are ready for use when quantum computing comes in the next couple of years.

Turn these pages for more on challenges and recommendations for CISOs.

Best of luck at GISEC 2023 and Ramadan Kareem for the holy month ahead.

RONAK SAMANTARAY

RONAK@GECMEDIAGROUP.COM

CYBER **SENTINELS**

PUBLISHER
TUSHAR SAHOO
TUSHAR@GECMEDIAGROUP.COM

EDITOR
SONAL CHHIBBER
SONAL@GECMEDIAGROUP.COM

CO-FOUNDER & CEO
RONAK SAMANTARAY
RONAK@GECMEDIAGROUP.COM

GLOBAL HEAD, CONTENT AND STRATEGIC ALLIANCES
ANUSHREE DIXIT
ANUSHREE@GECMEDIAGROUP.COM

GROUP SALES HEAD
RICHA S
RICHA@GECMEDIAGROUP.COM

PROJECT LEAD
JENNEFER LORRAINE MENDOZA
JENNEFER@GECMEDIAGROUP.COM

SALES AND ADVERTISING
RONAK SAMANTARAY
RONAK@GECMEDIAGROUP.COM
PH: + 971 555 120 490

DIGITAL TEAM

IT MANAGER
VIJAY BAKSHI

PRODUCTION, CIRCULATION, SUBSCRIPTIONS
INFO@GECMEDIAGROUP.COM

CREATIVE LEAD
AJAY ARYA

GRAPHIC DESIGNER
RAHUL ARYA

DESIGNED BY
THE C2S
DESIGN • MARCOM • BRANDING

SUBSCRIPTIONS
INFO@GECMEDIAGROUP.COM

PRINTED BY
Al Ghurair Printing & Publishing LLC.
Masafi Compound, Satwa, P.O.Box: 5613, Dubai, UAE

Office No #115
First Floor , G2 Building
Dubai Production City
Dubai
United Arab Emirates
Phone : +971 4 564 8684

GEC MEDIA GROUP

31 FOXTAIL LAN,
MONMOUTH JUNCTION, NJ - 08852 UNITED STATES OF AMERICA
PHONE NO: + 1 732 794 5918

A PUBLICATION LICENSED BY
International Media Production Zone, Dubai, UAE

معرض و مؤتمر الخليج العالمي لأمن المعلومات

GISEC GLOBAL

14–16 MAR 2023
DUBAI WORLD TRADE CENTRE

CONNECTING MINDS, BOOSTING CYBER RESILIENCE

> GISEC IS THE IDEAL CYBERSECURITY PLATFORM TO PARTICIPATE & PARTNER WITH ENTERPRISE & GOVERNMENT ENTITIES IN THE REGION.

H.E. DR. MOHAMED AL-KUWAITI
HEAD OF CYBER SECURITY
UNITED ARAB EMIRATES GOVERNMENT

SCAN ME

#GISEC.AE

ENQUIRE ABOUT EXHIBITING, SPEAKING & SPONSORSHIP
+971 (04) 308 6469 | GISEC@DWTC.COM | GISEC.AE

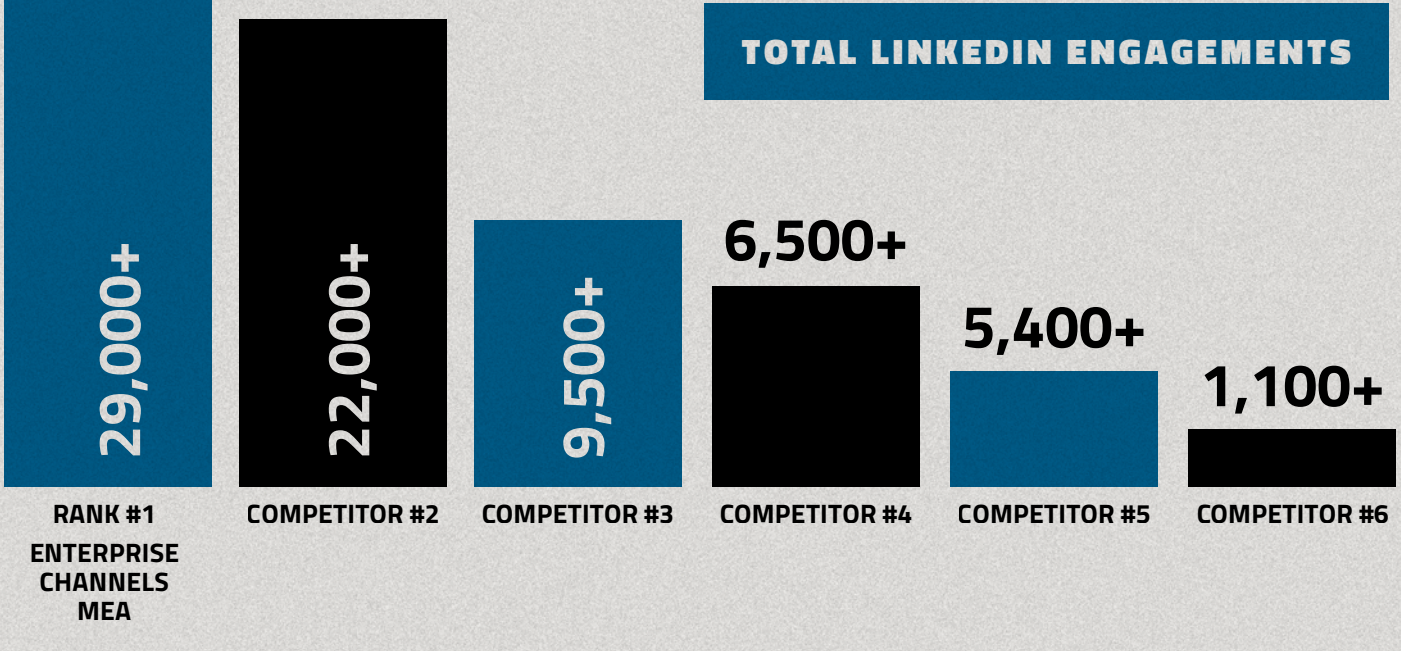
Officially Endorsed by
Official Government Cybersecurity Partner
Officially Supported by
Official Distribution Partner
Lead Strategic Partner
Platinum Sponsor
Gold Sponsors
Bronze Sponsor

CONTENTS

MARCH 2023

MOST ENGAGED IT CONTENT PORTAL ON LinkedIn

Enterprise Channels MEA thanks its LinkedIn communityfor making it the most engaged, local IT content portal in 2022.



PERIOD: 31 DEC 2021 TO 30 DEC 2022
SOURCE: LOCAL LINKEDIN ANALYTICS

SIX STEPS TO MITIGATE A RANSOMWARE ATTACK

Security leaders can reduce likelihood of ransomware attacks, reduce exposure to vulnerabilities, secure the organisation using a mitigation plan.

Paul Webber, Senior Director Analyst, Gartner.

Ransomware can cost companies millions of dollars, and a potentially even greater loss over the long term, impacting reputation and reliability. In recent cases of ransomware attacks, the victim organisations have paid huge amounts to the attackers, which can be one of the reasons these attacks are getting more popular.

Instead, what organisations need to focus on is preparation and early mitigation if they want to cut losses to ransomware. Key people such as the CEO, board of directors and other important stakeholders must be involved in the preparation. In the event of a ransomware attack, it is likely that journalists and other external stakeholders will reach out to the board of directors for response to the attack, not the security leaders or CISO.

This plan must cover the following six actions.

> "Key people such as the CEO, board of directors and other important stakeholders must be involved in the preparation"

#1 Conduct ransomware assessments

Conduct risk assessments and penetration tests to determine the attack surface and current state of security resilience and preparedness in terms of tools, processes and skills to defend against attacks. Before you assume that payment is the only option, investigate using free ransomware decryption software.

#2 Enforce ransomware governance

Establish processes and compliance procedures that involve key decision makers in the organisation, even before preparing for the technical response to a ransomware attack. Ransomware can escalate from an issue to a crisis in no time, costing an organisation revenue loss and creating a damaged reputation.

#3 Maintain operational readiness

Conduct frequent exercises and drills to ensure that systems are always able to detect ransomware attacks. Build regular testing of incident response scenarios into the ransomware response plan. Test, test and retest at regular intervals to check for vulnerabilities, noncompliant systems and misconfigurations. Ensure that incident response processes are not themselves reliant on IT systems that may be affected by ransomware attacks or unavailable in case of a serious incident.

#4 Backup, test, repeat ransomware response

Back up not only the data but also every nonstandard application and its supporting IT infrastructure. Maintain frequent and reliable backup and recovery capabilities. If online backups are used, ensure that they cannot become encrypted by ransomware. Harden the components of enterprise backup and recovery infrastructure against attacks by routinely examining backup application, storage and network access and comparing this against expected or baseline activity.

#5 Implement least privileges

Restrict permissions and deny unauthorised access to devices. Remove local administrator rights from end users and block application installation by standard users, replacing this with a centrally managed software distribution facility.

#6 Educate and train users

Research government and regional authorities that have provided guidelines on how organisations can fortify their network infrastructure against ransomware. CISOs and security leaders can use guidelines such as these to create a basic training program for all staff in the organisation. However, ransomware preparedness training needs to be customised to the organisation for better results.

Use cyber crisis simulation tools for mock drills and training that provide closer to real-life situations for better preparedness of end users against ransomware, says Webber.

The challenges of ransomware and other forms of malware are the ever-changing tactics and agendas of hackers. Having a strategy in place for preparedness can help contain the losses and protect the organisation.

AI+ML MUST BE EMBEDDED INSIDE THE SECURITY STACK

AI moves systems towards decision making, while ML churns data rapidly looking for patterns, improving capability and speed to block any threat actor.

Tamer Odeh, Regional Sales Director, SentinelOne.

Hybrid work cultures have tremendously expanded the attack surfaces of enterprises. Tactics, techniques, procedures of modern-day threat actors have become rapid and highly sophisticated. Previously rated as advanced techniques in ransomware, crypto jacking, phishing, software supply chain, are now becoming mainstream.

While the cybersecurity industry is continuously innovating its solutions to improve performance, reduce cost and complexity, and match market requirements, so is the exploding industry of developing threat malware and availability of threat actor competency. While enterprise IT end users use Anything-as-a-Service to manage their operational challenges, so does the threat actor enterprise.

Net result is that the task expectation and level of challenge for the chief information security officer, CISO in enterprises is going through the roof. The solution for many CISOs is now to move away from dependence on a single solution and to build solution stacks, closing gaps and loopholes and overlapping strengths.

The single-layer, reactive based solutions are no longer adequate to face modern day, advanced threat actors.

Bringing in artificial intelligence tools and using machine language frameworks around volatile datasets is increasingly being accepted as the way forward now. In tandem these two platforms accelerate and automate rapid decision to identify, respond, manage and scale with the threat actor global syndicate.

Artificial intelligence makes compute system behave like a human, while machine language churns data looking for patterns, takes decisions, prioritises actions, and this isolates threat malware.

In May 2022, the U.S. Senate Armed Forces Committee's Subcommittee on Cyber held a congressional hearing on the importance of leveraging artificial intelligence and machine learning within the cyberspace. The committee highlighted a growing concern about shortfall of technically trained cybersecurity personnel across the country in government and industry alike. The global shortage of 2.7 million cybersecurity roles is concerning.

The shortage of cybersecurity skills is what is overwhelming the CISO and cybersecurity department, in other words the alert to response ratio. Artificial intelligence and machine learning can enhance their capability giving them breathing space to strategize.

> "While enterprise IT end users use Anything-as-a-Service to manage their operational challenges, so does the threat actor"

Amongst the other benefits:

- Artificial intelligence tools can process thousands and millions of vector data per second in real time
- Patterns of emerging attacks can be detected in real time by artificial intelligence
- Human patterns in vector data are detectable and predictable by artificial intelligence
- Without artificial intelligence, large scale, moving data sets are not actionable or useful not humans
- Artificial intelligence can build a complete threat analysis model that is the basis for setting up a Zero Trust framework
- Artificial intelligence can benefit cybersecurity teams by automating interpretation of the vector data
- Artificial intelligence can benefit cybersecurity teams by automating prioritisation of alerts and flagging of incidents detected in the vector data
- Artificial intelligence can adapt to changes in the vector data as the scale and speed of the threat actor changes

In summary a combination of artificial intelligence and machine language does not just identify malware and threats. It searches real-time data for changing patterns, old and new tactics and identifies threats in the early stages. This lowers the mundane task level for the triage team including analysts and SOC managers. Moreover, automation can help to set up differentiated response levels based on the nature of the device and data associated with any incident.

PERMANENT PROTECTION FOR DATA THROUGH IMMUTABILITY

This means storing backups in an immutable, read-only manner and prevents all data and backups from being encrypted if infiltrated by ransomware threat actors.

Rick Vanover, Senior Director Product Strategy, Veeam.

73%, that is the percentage of organisations that have been affected by at least two ransomware attacks in the past year, according to the Veeam Ransomware Trends Report 2022. In most cases, the criminals' path into the corporate network leads through the weakest element of the digital defence: humans.

Phishing remains the means of choice for hackers and data thieves to gain unauthorised access - as confirmed by the latest Verizon Data Breach Report. While backups are often able to act as a last bulwark against extortionists, the right credentials can crack even this bastion. As a result, companies must become increasingly aware that their own employees also pose an unwanted threat. The best way to manage this risk is through Zero Trust.

Zero Trust is not a standalone product, but a paradigm that is woven into the corporate culture. IT administrators must weigh which employees should have access to which content, applications, networks and data. This goes double for storage, because: Backups are, in many situations, the lifeline that can keep companies running. However, if this anchor is damaged, downtime increases rapidly and recovery is made nearly impossible.

> "Options for setting up an immutable backup range from air-gapped solutions to AWS S3 Object Lock"

Therefore, roles and rights related to storage must be assigned with appropriate caution. Only dedicated staff and storage administrators should have the ability to access backups. But what happens if a user account of these very administrators falls into the wrong hands?

The only way to permanently protect backups from the wrong hands is immutability. In the area of storage, this means storing backups in an immutable, read-only manner, so to speak. This prevents all data and backups from being encrypted even in the event of infiltration by ransomware groups, for example. The options for setting up an immutable backup range from air-gapped solutions to the AWS S3 Object Lock - arguments for the different variants can be found quickly.

However, it is important that they are implemented as a fixed part of the backup strategy. This guarantees that the reassurance provided by backups remains intact throughout if access falls into the wrong hands, and data can always be restored in the event of an emergency.

> "If this anchor is damaged, downtime increases rapidly and recovery is nearly impossible"

Implementing Zero Trust in storage is a process that takes time and then needs to be looked at regularly to ensure continuous security. Phishing will certainly continue to be one of the biggest threats to organisations and their data, as the employee will remain the biggest risk to the defence. However, if roles and privileges have been assigned according to the zero-trust paradigm, then you minimise that risk as much as at all possible. This keeps backups the bulwark against ransomware that they are supposed to be.

NEVER TRUST, ALWAYS VERIFY IS GISEC 2023 THEME

Middle East governments and corporates are expected to invest heavily in Zero Trust Access, ZTA IT systems over the coming years to ward off the omnipresent threat of cyber-attacks, providing a major boost to the region's cybersecurity market that's predicted to more than double in value over the next five years.

Exhibitors at Gisec 2023, said ZTA security – an approach to designing IT infrastructure with a never trust, always verify model – will be highly sort after in 2023 and beyond, as organisations seek to protect their data and systems against constantly evolving and increasingly sophisticated cyber threats.

In the Middle East, the pervasive work from anywhere culture is convincing companies to double down on their efforts to protect digital assets, fuelling the region's cybersecurity market that, according to analysts Markets and Markets, will grow from $20 billion in 2022 to $45 billion in 2027, clocking 17% annual growth.

Rising IoT traffic, increasing technological advancements and modernisation of enterprises are also fuelling demand for zero trust security solutions, with MarkNtel Advisors, a research company, expecting the Middle East ZTA market to grow by 16% annually over the next five years.

The core cybercrime methods have not changed, but the sophistication of them has increased. The good news is IT security professionals and C-level decision makers will have no shortage of solutions to investigate at Gisec 2023.

Household names such as tech titans Huawei and Microsoft will be out in full force at the annual three-day event, alongside headline ground-breaking infosec companies including Spire Solutions, CPX, Mandiant, Pentera, Cloudfare, Crowdstrike, Edgio, Secureworks, Synack, Threatlocker, and Votiro.

"In our increasingly digital world, security is a key concern and area of focus," said Waseem Hashem, Business Group Director for Modern Work and Security at Microsoft UAE. "At Microsoft, we have a long-standing commitment to securing our platforms and providing solutions, and our answer to safeguarding the digital space in the face of evolving threats is the Zero Trust network and architecture."

"Businesses worldwide are prioritising secure and efficient network access, making the adoption of Zero Trust non-negotiable. In the Middle East, in particular, where cyber threats

The region's cybersecurity market according to Markets and Markets will grow from **$20 billion** in 2022 to $45 billion in 2027 at 17% growth

are becoming more persistent and sophisticated, the implementation of this approach is a critical step for organisations to protect their sensitive data."

CPX, a home-grown cyber security entity based in the UAE, will this year showcase its complete suite of end-to-end cybersecurity capabilities covering all industries from energy and utilities to government and defence, healthcare, finance and transportation.

Commenting on the Zero-Trust networks, Paul Lawson, Executive Director at CPX, said, "The fast-paced growth of emerging technologies like AI, ML, Cloud and IoT has put a strain on an organization's ability to secure, protect and mitigate looming cyber threats."

"We expect these shifts to significantly contribute to a rise in the adoption of Zero Trust models. A Zero Trust approach distrusts all entities by default, requiring all users inside and outside a network to be continuously authenticated and authorised."

"In the Middle East, many organisations still depend on a traditional firewall-based perimeter architecture. As organisations embrace new advanced technologies and frequently migrate to Cloud, they should align and enhance their cybersecurity posture by deploying Zero Trust aware technologies."

Zero Trust to replace VPN

Another key factor behind the growth of ZTA is the increasing adoption of cloud technologies, leaving organisations migrating workloads to the cloud increasingly vulnerable to wily attackers, posing major challenges and causing significant losses.

Tech research firm Gartner predicts that zero trust network access will even replace virtual private networks, VPNs by 2025, with the rise in remote work and the continuing threat of cyber-attacks urging companies to scout for more robust security frameworks.

Says Anil Bhandari, Chief Mentor at ARCON – a cybersecurity provider with sales headquarters in Houston, Texas – organisations are gearing their investments towards a system that, among several characteristics, uses multi-factor authentication to verify the identity of users and devices.

"According to our research, adopting zero trust networks and architecture will be a top priority for IT security executives in the Middle East and around the world this year," said Bhandari, who will be at Gisec Global 2023 with ARCON's Converged Identity Management platform – a Software as a Service identity and access management platform.

"In the Middle East, in particular, for a typical large-scale enterprise or mid-size company, the IT perimeter is no longer confined to on-premises data centres. As modern-day IT infrastructure is large and distributed in hybrid and multi-cloud setups, Middle East IT security leaders will look to build micro-segmentation and micro-perimeters for controlling and securing digital identities."

Think Zero Trust

CyberKnight, a UAE-based cybersecurity value-added-distributor will meanwhile have a dedicated Think Zero Trust theme at Gisec Global 2023, with CMO Olesya Pavlova, stating that attackers are continuously expanding their capabilities and taking advantage of an ever-growing number of attack vectors.

"In 2022, we saw that cybercriminals targeted Middle East critical infrastructure, including information technology, financial services, healthcare, and energy sectors, with headline-grabbing incidents," said Pavlova, whose CyberKnight recently partnered with American zero trust real-world cybersecurity company Xage to accelerate ZTA adoption across the Middle East."

"Currently, we see XDR, data security, threat intelligence and application security with the highest demand. Our purpose remains the same going forward – to help fight cybercrime using Zero Trust."

Elsewhere, US-based StrikeReady will showcase its award-winning AI-powered Cognitive Security Platform at Gisec Global 2023. AI capabilities such as reinforcement learning, natural language understanding, and proactive conversational AI enable StrikeReady's Cognitive Security Platform to offer innovative features such as a virtual cybersecurity assistant.

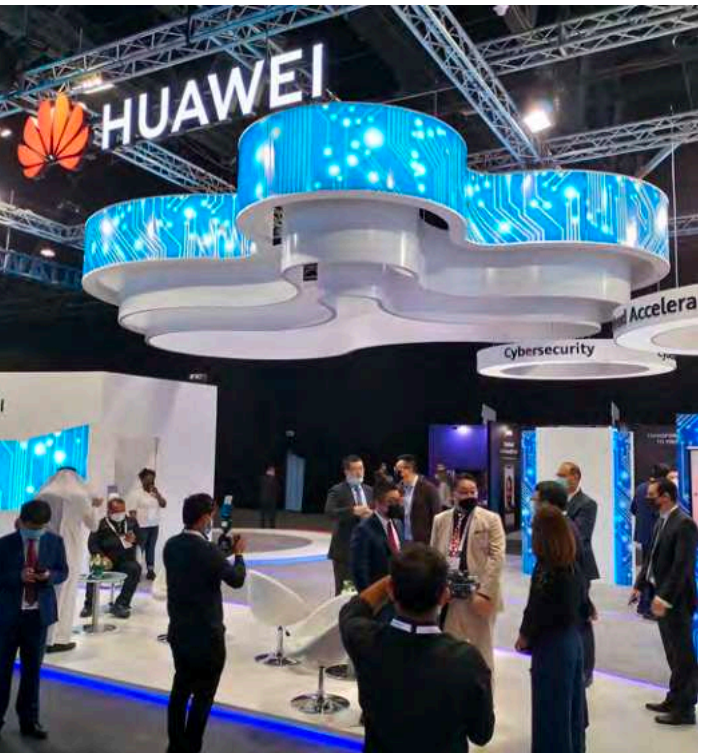
Anurag Gurtu, Chief Product Officer at StrikeReady, said in order to continue to evolve in the same way that attackers do, thriving organisations must have ZTA as part of their cyber security transformation.

"The Middle East is one of the few regions that adopts cyber security early, so I suspect many businesses there have looked into ZTA," said Gurtu. "Attackers are innovative, and their tactics continue to evolve to defeat existing cyber defences. It is imperative that the industry adapts and evolves in order to stay competitive with attackers."

Gisec Global has an extensive conference programme under the theme Connecting minds, boosting cyber resilience, with 13-tracks tackling the evolving cyber landscape and corresponding threats across multiple industries.

"The Zero Trust model addresses the Middle East's growing concern of cyber-attacks on critical infrastructure, while providing a more comprehensive approach to security by requiring verification of all users and devices, regardless of location, and implementing strict access controls," said Riju George, Group Director for Gisec at DWTC.

Gisec 2022 recap




cisco


ITB
IT Cyber Security
OT Cyber Security
DRAGOS
DRAGOS


Qualys.
Continuous Security
Qualys
One Platform
Qualys
One Platform.
One Agent.
One View.
Now bringing the unified power
of the Qualys Cloud Platform to ED

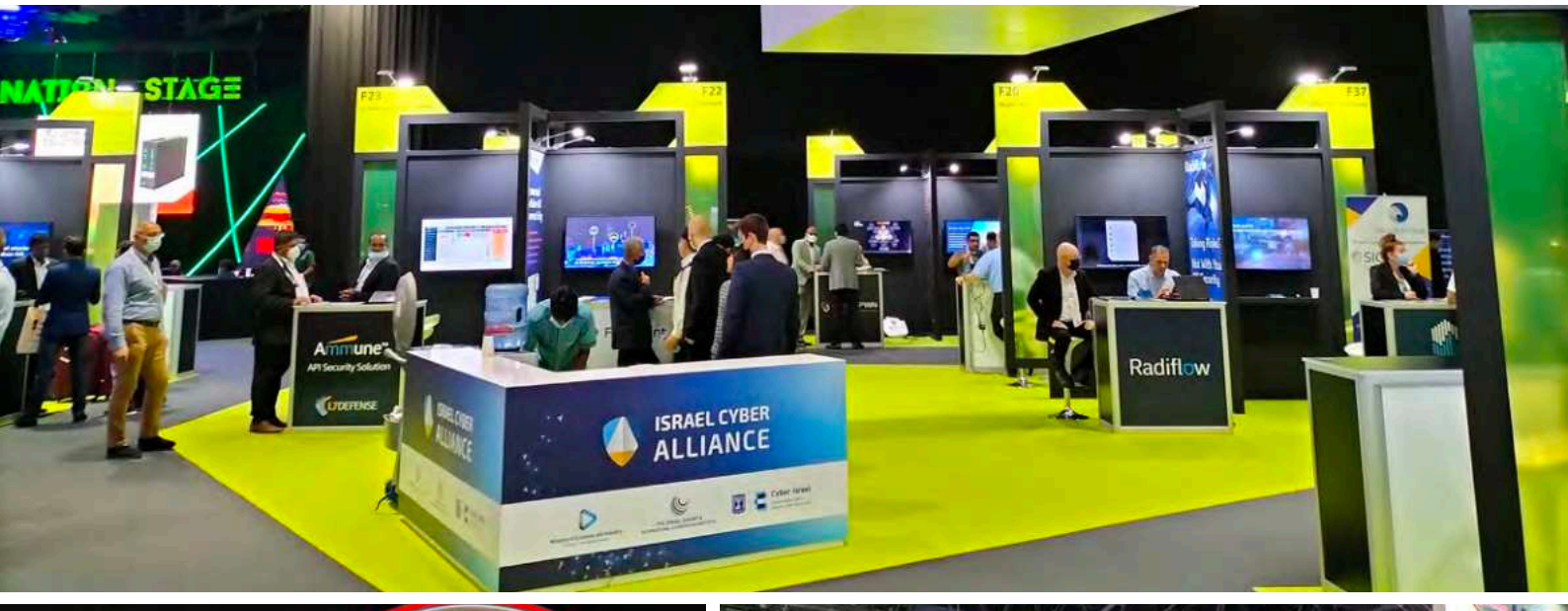

tenable
tenable
SEE
EVERYTHING
PREDICT

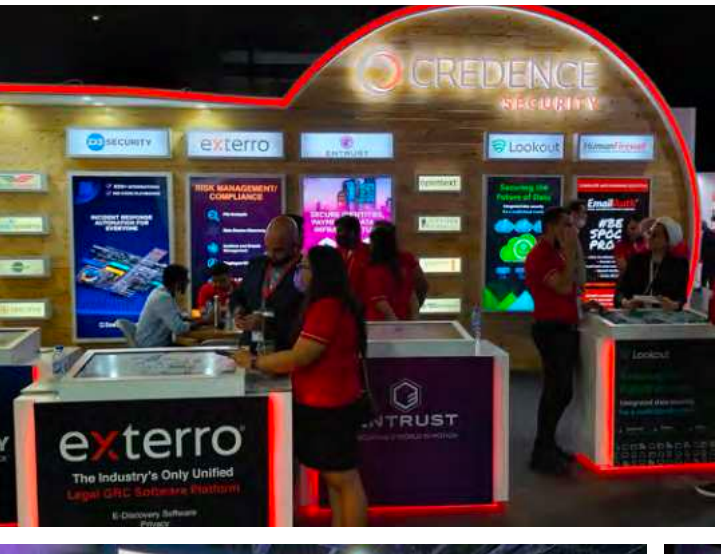

and Visibility
nozominetworks.com
D32
The Leader in OT & IoT Security and Visibility
Leadership in
Key Industries


Microsoft
Microsoft


emt
TECHNOLOGY DISTRIBUTION
SECURITY | CLOUD | ICT MANAGEMENT
eEngine


ARMIS
Our Portfolio
Data Security
netwrix
SECLORE
People Identity & Security
Attivo
Ilantus
IMMERSIVELABS
Device Security
Lookout
ARMIS.
Network Security
BLUECAT
IronNet
appgate
Workloads & Application Security
illumio
checkmarx
Visibility & Analytics
REDSEAL
GROUP-IB
ARISTA
solarwinds
Automation & Orchestration
CYWARE
seceon
STRIKE READY


STAGE
Armmune
API Security Solution
DEFENSE
ISRAEL CYBER ALLIANCE
Radiflow

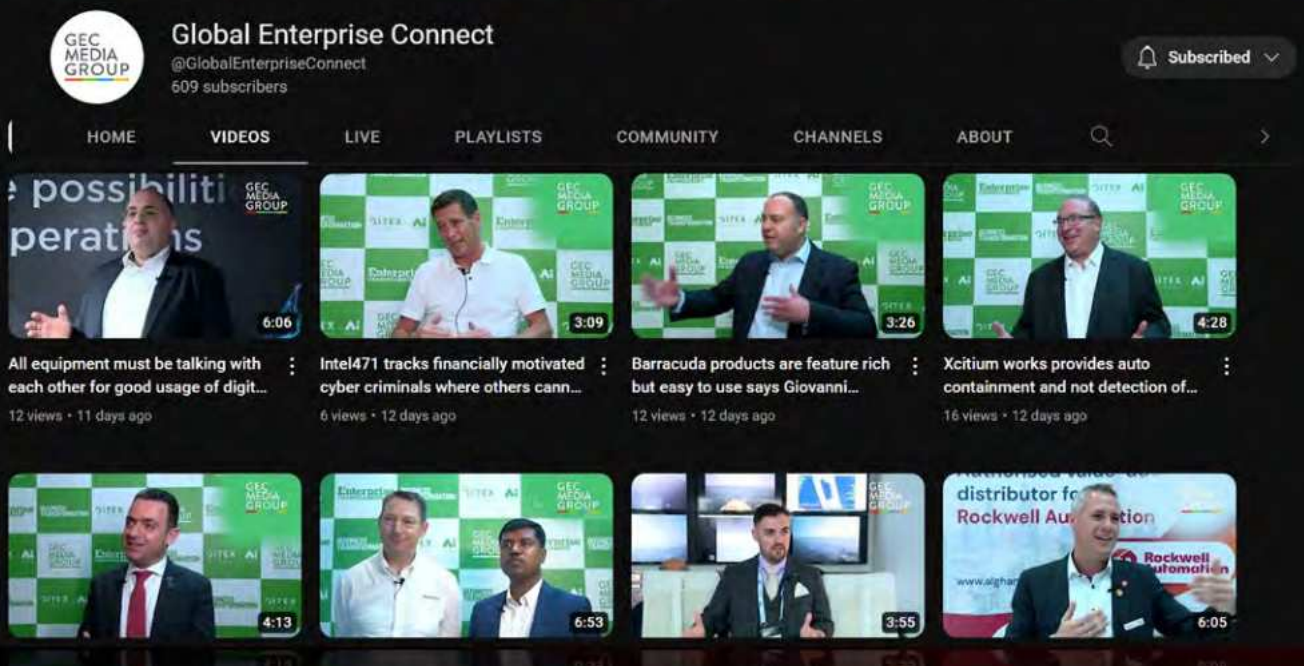

CREDENCE
SECURITY
exterro
Lookout
exterro
The Industry's Only Unified
Legal GRC Software Platform


HAVELSAN
TURKISH CYBER SECURITY CLUSTER
TRT


ITB


EXIT

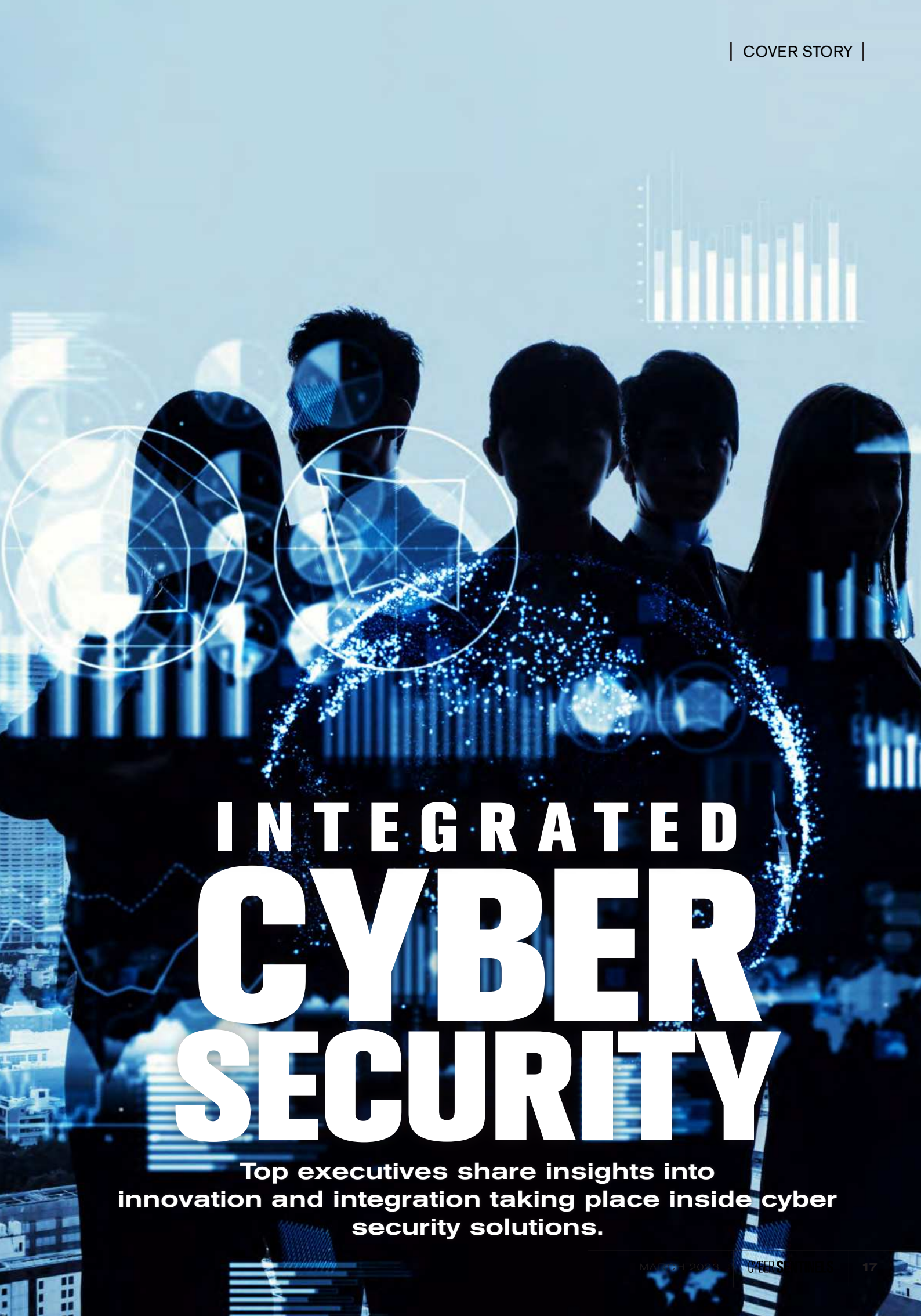
Gisec 2022 recap



SUBSCRIBE NOW

To our video channel for latest updates

GEC MEDIA GROUP



INTEGRATED CYBER SECURITY

Top executives share insights into innovation and integration taking place inside cyber security solutions.

BeyondTrust

MOVING BEYOND VANILLA SECURITY AND TRUST

Organisations must adopt solutions that allow security teams clear visibility into identities and reveal their impact on the security posture.

A CISO lives in a world that is constantly changing. From static environments that have new attack vectors to underlying changes in infrastructure, workflows, and processes in which new mechanisms for security must demonstrate regulatory compliance controls, a CISO has to deal with all of them. And the challenges and pains apply to both, protecting what is established from the evolution of attacks to designing, installing, and monitoring security for what is new.

For enterprises and their CISOs, it can be a challenge to secure old systems from modern attacks and a pain to design new systems that do not introduce unnecessary risk. In the real world, these are real security issues in 2023. BeyondTrust listed several threats that organisations should worry about.

Firstly, organisations can expect a new round of attack vectors that target and successfully bypass Multifactor Authentication or MFA strategies. Push notifications, and other techniques for MFA will be exploited, just like SMS. Organisations should expect to see the foundation of MFA eroded by exploit techniques that compromise its integrity and require a push for MFA solutions that use biometrics or FIDO-2-compliant technologies.

Second, attackers will lean more on their powers of persuasion than on their malware kits as they step up social engineering attacks in the cloud. A single fake social media profile, leveraged in the right way, can allow a threat actor to gain employment or impersonate a trusted vendor. This trend will call for more rigorous background checks and communications that rely on more than just a simple social media profile.

Using open-source intelligence or OSINT, threat actors will exploit social media to trick unsuspecting victims. Suitably anonymised, the threat actor can persuade victims to divulge secrets or act in other ways contrary to their interests or that of their employer. The Lapsus$ group used social media to become an employee and then spoof access by calling a support helpdesk.

At the end of 2022, BeyondTrust announced Identity Security Insights, ISI. With the explosion of human and machine identities and the proliferation of new access paths to critical systems and data, organisations have been left with poor visibility into identity threats and other identity-related security exposures. BeyondTrust's new solution empowers security teams with clear visibility into all identities, privileges, entitlements, permissions, rights and access and reveals their exact impact on the organisations' security posture.

The solution also provides intelligent, actionable analytics that any organisation can leverage to immediately improve security posture and eliminate potentially dangerous backdoors and weak spots based on identity and account compromise. It brings the concepts of Identity Detection and Threat Response or IDTR which is designed to protect identity as the new perimeter.

In May last year, the company announced its all-in-one global programme. The enhancements included the introduction of MSP, GSI and Service Delivery Partner tracks to complement the existing reseller track. The enriched and refined, all-inclusive programme removes region-specific requirements and benefits and discount structure for partners.

The global approach simplifies all partner and BeyondTrust interactions, allowing the channel managers and partners to devote more time to developing strategic, mutually-beneficial sales plans. As they grow their business, the Authorised, Silver and Gold partners in Europe, the Middle East, India and Africa regions will also see increased programmatic discounts for deal registration, providing them with the opportunity to make higher margins.

Morey Haber, CSO, BeyondTrust.

- Create systems to protect against established threats and design, install, and monitor security for what is emerging ones.
- Use a solution that provides intelligent, actionable analytics to eliminate potentially dangerous backdoors and weak spots.
- Expect a new round of attack vectors that target and successfully bypass MFA strategies and exploit push notifications.

Cloud Box Technologies

ENABLING SECURITY FOR EMERGING THREAT MODELS

AI is transforming businesses, adding resilience and cutting-edge technology for good, but it is also increasing the complexities.

Biju Unni, Vice President, Cloud Box Technologies.

The new SEC, Securities and Exchange Commission, regulations are influencing the ever-changing security landscape. There is a strong emphasis on sustainability which would require businesses to relinquish the carefree attitude and think about concrete steps to be in line with the SEC. The localisation laws would get the global players to pivot from a global scale to a local scale but also give the local companies traction to get into the data space. These regulations are primarily aimed at preventing identity theft and also improving cybersecurity.

Localisation helps local companies develop specific skill sets with pertinent local knowledge and this goes a long way to improve the customer experience and enhance satisfaction. The regulations also prompt companies to take a deep look at the present and improve the future.

Intelligence in the security domain is a fast-changing unit with varying subunits. The ever-progressing Artificial Intelligence or AI has considerably improved security but has also provided pain points for security vendors with its adoption by threat actors. These changes are reflected in the security product portfolio of Cloud Box Technologies which incorporates all required changes and improvements.

There is a close link between automation and intelligence and sectors like banking, financial services, and insurance or BFSI and retail are proactively adopting it. Automation develops in sync with robotics and they are quite visible in the marketplace. The hybrid cloud paradigm is rapidly becoming a norm in infrastructure and companies are actively looking at new models. This also resonates well with the security scenario. Solutions now come in hyper-convergent forms and smart platforms are the new preference for the industry. This goes well with our strategy of providing value across multiple technologies.

The security product portfolio of Cloud Box incorporates all required changes and improvements

Protecting organisations from the myriad of cyber threats and challenges is the most important role of the CISOs and security leads. One of the foremost challenges in this position is the need to evolve with technology and the threat landscapes. This needs to be continuous to understand that the role is all about risk mitigation and not risk elimination. The need to manage the team, the human factor, does require soft skills and is very critical to the overall result. The need to build resilience, to cope with the attack vectors and surfaces and their frequency is paramount for any CISO.

AI has transformed businesses for the good and added resilience and cutting-edge technology to all IT domains including the most important one, security. However, it has also contributed to the increasing complexities of threats. Ironically, the threat actors have actively adopted AI as well. This coupled with the seeming reluctance of CIOs to buy into the threat cognisance severely hinders risk mitigation and helps the threat actors.

Going ahead, more threat models will manifest and organisations will have to be well-prepared for different scenarios.

FOR CISOs

- Businesses must evolve with technology and the threat landscape.
- Build resilience, to cope with the attack vectors and surfaces.
- Proactively adopt automation and intelligence to improve security.
- The hybrid cloud paradigm is rapidly becoming a norm and it resonates well with the security scenario.

Delinea

EXTENDING PRIVILEGED ACCESS MANAGEMENT

By treating all users as privileged, extended PAM enables policy-based authorisation, Zero Trust, and least privilege best practice.

Mohammad Ismail, Regional Director Middle East, Delinea.

In the post-pandemic digital world, most companies are cloud-based with a mix of human and non-human machine identities and an ever-growing list of disparate, fragmented security solutions that lack coordination and consistency. As a result, security is full of blind spots, making it difficult to anticipate and combat evolving attacks against privileged accounts.

To accommodate these security challenges and operational expectations, Privileged Access Management or PAM is evolving into what is called Extended PAM, which treats all users as privileged users and relies on policy-based authorisation controls to establish Zero Trust and least privilege best practice.

Extended PAM involves establishing data-backed policies and controls to prevent bad actors from moving laterally and escalating privileges, making privileged access more intelligent. It also allows setting up analytics-informed policies to assess the changing conditions and adapt access where and when necessary, saving IT and security departments time in managing access while improving security.

The global survey of cybersecurity leaders found that in the UAE and Saudi Arabia, a staggering 91% of respondents reported that they experienced an identity-related breach or an attack using stolen credentials during the previous year and a half.

While the importance of identity security is acknowledged by business leaders, most of the interviewees said they will not receive the backing and budget they need to put vital security controls and solutions in place to reduce major risks. This means that the majority of organisations in the region will continue to leave privileged accounts vulnerable to cybercriminals looking to abuse them. This includes 'non-human' identities, which are growing at a faster pace than human users. Overlooking them increases the risk of privilege-based identity attacks.

One of the most interesting developments the industry witnessed through 2022 was a 61% decline in the number of organisations that were victims of ransomware attacks compared to the previous year. Delinea's State of Ransomware survey report also found that the number of companies that paid the ransom declined from 82% to 68% during the previous year.

Ransomware has, for several years, been a top cybersecurity concern and although these decreasing figures relate to the US, they indicate that organisations are becoming more resilient. At the same time, one must stay wary of becoming complacent. The research revealed that budget allocations for ransomware are in decline.

Overall, according to the survey report, only 68% of organisations are currently allocating budgets to protect against ransomware as compared to 93% during the previous year. Besides, only 51% of them indicated that they are taking proactive, proven steps to prevent ransomware attacks such as enforcing password best practices while 50% said they are using Multi-Factor Authentication.

As a company, Delinea strongly believes that partner programmes should be designed to be simple and seamless. The focus this year, therefore, is on ensuring that the programme's benefits and value can be clearly understood by its partner community.

Moreover, with customers under constant pressure to optimise budgets and becoming more discerning about their IT spending, partners can expect to benefit from the company's commitment to enabling them to work better together with the direct sales teams so the full value proposition of Delinea solutions can be effectively demonstrated.

FOR CISOs

- Establish data-backed policies and controls to prevent bad actors from moving laterally and escalating privileges.
- Set up analytics-informed policies to assess the changing conditions and adapt access where and when necessary.
- Focus on 'non-human' identities to reduce the risk of privilege-based identity attacks.

Entrust

DELIVERING SECURITY SOLUTIONS FOR PEACE OF MIND

A key challenge for 2023 will be tackling imminent protection and threats, while future-proofing for short- and mid-term developments

Simon Taylor, Channel Sales Director MEASA, Entrust.

Although data privacy guidelines in the region are not bound to SEC regulations, they certainly have global influence. As the region, led by government initiatives, strives to be a leader in cybersecurity and data protection, it is important to look at international regulations, such as those imposed by SEC, as best global practices.

Additional compliance-based regulations are already being implemented across GCC and data privacy policies will continue to grow stronger in the coming years. The SEC regulations might not have an immediate legislated impact but the strongest and most perceptive teams will be working toward achieving this level of governance.

Entrust protects data and the individuals who access it, including both humans and machines. For some time now, Entrust has been moving away from segmented product offerings towards a comprehensive ecosystem allowing customers to protect data and individual assets within one solution set. By doing so, Entrust sets itself apart as the only security vendor to offer universal protection across an organisation's product group.

Automation is key to data protection, with human error being one of the strongest threats to data security. For example, Entrust's Identity as a Service or IDaaS is a tool that offers a cloud-based solution with a zero-trust approach to security, making it easier for users to be compliance-bound to prevent data loss and data breaches.

A key challenge for 2023 will be balancing the processes for tackling imminent protection and threats, while future-proofing for short- and mid-term developments. Foreseeing risks and planning for long-term data protection is becoming increasingly important. For example, teams need to be designing systems that are ready for use when quantum computing comes in the next couple of years, as the existing algorithms won't stand up to a post-quantum world. Data from the National Institute of Standards and Technology indicates that this is much closer than many think. The ability to be agile and future-proof amidst ongoing budgetary challenges will be the key to successful long-term data protection.

The Middle East is one of the most highly attacked regions, with the use of malware and other processes to try and gain data. The financial sector in particular is the hardest hit sector for GCC, but other sectors, such as healthcare, which is the most targeted industry globally, are beginning to adopt best business practices. As the shift towards cloud adoption continues, there is a need to bolster cybersecurity.

Entrust is already witnessing an uptick in requests for assistance across the protection tools in 2023 and this is expected to continue with companies looking to grow and strengthen their data protection. The company has one of the largest partner programmes available, utilising a huge amount of its research and in-depth knowledge to create invaluable protection tools. Companies no longer have to patch together solutions using multiple vendors because Entrust can handle it all to deliver a simple solution and peace of mind.

Data security is about agility and Entrust is constantly working toward improving and expanding its portfolio through acquisition and research and development to be future-proof. It serves as a one-stop shop for the protection of individual and machine data.

FOR CISOs

- Look at international regulations, such as those imposed by SEC, as best global practices.
- Create a balance in processes for tackling imminent threats, while future-proofing for short- and mid-term developments.
- Design systems that are ready for use when quantum computing comes in the next couple of years.

Equinix

DEPLOYING DIGITAL-READY NETWORK INFRASTRUCTURE

Equinix helps customers accelerate performance with lower latency without the need to make investments in large hardware stacks.

The regulatory landscape continues to evolve, and business leaders must consistently invest in the skills and technology to keep updated. The key is to take advantage of digital ecosystems and stay on the right side of data privacy laws. Ecosystems have become essential to business success, whether it is collaborating with partners to drive innovation or tapping into

Platform Equinix can provide the infrastructure needed to get close to partners and customers at the edge

Kamel Al-Tawil, Managing Director, Middle East and North Africa, Equinix.

the cloud and Software-as-a-Service providers for greater performance and new services on demand. Businesses must balance their compliance requirements against the need to share data across their digital ecosystems.

Digital leaders today are setting up the digital transformation process by optimising their digital infrastructure. They're doing this because they know they need a strong platform to build capabilities that increase their efficiency and agility.

Platform Equinix can provide the infrastructure needed to get close to partners and customers at the edge, no matter where the digital transformation ends up taking someone. In addition, its portfolio of interconnection services, including Equinix Fabric which offers secure, software-defined interconnection from anywhere across our global footprint, makes it easier to tap into the digital services that fuel business transformation.

Digital services like Equinix Network Edge enable businesses across multiple industries to transform their network and deploy digital-ready infrastructure at the edge with ease. Further reduction in complexity, cost and management strain helps businesses set up highly available applications at closer proximity to customers, employees, partners, and ecosystems.

One challenge that businesses face is the complex and rapidly changing security landscape. With cyberattacks increasing in both frequency and intensity, IT leaders must pursue their digital transformation priorities without increasing cybersecurity risk. To do this, they need a holistic security strategy that protects both their digital assets and their physical infrastructure. Preventing data breaches is a particular area of concern, both because of the data protection regulations and the high costs and reputational damage that inevitably follow such incidents.

Virtual digital twins enhance productivity and development times for products, with substantial financial savings

Equinix Fabric helps keep data protected in transit. Enterprises can bypass the public Internet to form direct, private connections to any of the customers. This allows them to move sensitive data anywhere it needs to go without exposing it to cyberattacks. Given this dynamic digital transformation landscape, several prevailing drivers will accelerate and power digital infrastructure deployment and consumption over the next decade.

Emerging technologies are at the forefront of innovation. Newer technologies like Artificial Intelligence, 5G and the Internet of Things, are improving operations and accelerating the development of new products, including autonomous cars, smart cities, augmented reality, and more. However, applications of these technologies already process tremendous volumes of data, and this trend is only going to accelerate.

To take full advantage of the opportunities emerging technologies present, organisations need a flexible hybrid infrastructure that gives them the agility to dynamically adapt to changing business requirements. The emergence of 5G technology promises to offer unprecedented, always-on and nearly instant access to content, data resources and yet-to-be-created interactive services, all with real improvements in capacity and performance.

The era of digital twins has now arrived where organisations can create virtual copies of their factories, hospitals, datacentres, aeroplanes, supply chains, etc. to monitor and maximise potential. Virtual digital twins enhance productivity and development times for products, with substantial financial savings.

Organisations have accelerated their decision-making when investing in modernising and transforming their IT infrastructure. The increasing demand for multi-vendor solutions is fuelling the growth of the channel market as organisations look for comprehensive IT infrastructure and solutions to help them meet complex business challenges.

A crucial element of Equinix's changing business model is the growing emphasis on aligning with partners to position its partner ecosystem for success. With Equinix's digital service offerings around Network Edge and Equinix Metal, and the interconnection platform with Equinix Fabric, the company helps customers accelerate performance with lower latency and reach new markets without having to make large investments into a large stack of hardware.

Equinix Network Edge enable businesses across industries to transform their network and deploy digital-ready infrastructure

- IT leaders must pursue their digital transformation priorities without increasing cybersecurity risk.
- Adopt a holistic security strategy that protects both digital assets and their physical infrastructure.
- Build flexible hybrid infrastructure that can dynamically adapt to changing business requirements.

GBM

PROVIDING INTEGRATED, VENDOR-AGNOSTIC SECURITY

Organisations need managed security offerings that can cut through the noise and help businesses to focus on high-value assets.

Hasanian Alkassab, Senior Regional Security Manager, GBM.

Governments and regulators have been setting up formidable compliance requirements to protect their constituents and customers. Complying with these regulations requires dedication and intricate familiarity with the region.

It is also important to understand the guidelines for disclosing data breaches, how the information can be shared so that everyone can learn from these incidents, and how organisations are being held accountable for data breaches. There are also internal and external factors that are crucial for data security and privacy and can have an impact at the regional level.

As one looks at these factors, one can see the growing trend of demand for managed security offerings that enable companies to cut through the noise, focus on their most high-value assets, and address the more relevant risks to their specific business.

The presence of automation and Artificial Intelligence, AI in fending off cyberattacks has become a very real thing. This is something that has been embraced by GBM in its offerings with the launch of the Cyber Defence programme, including the GBM Shield and the acquisition of Cor., a Coordinates platform that enables integration, automation, and orchestration across any technology to provide defence-grade services to enterprises of all sizes.

With its disruptive approach to cyber defence, the GBM Shield programme boosts the ability to anticipate, detect and respond to cyberthreats. It delivers something unique, as they try to focus on making sure to augment the technology and the human skills within their clients to use Machine Learning and AI so that humans can focus on the top issues that need to be examined and take action on them. GBM will be showcasing these solutions, and more, at this year's GISEC.

Even though awareness of cyberthreat is high at the regional level, the attacks keep getting more sophisticated. For CISOs and security decision-makers, new challenges are constantly emerging as the cybersecurity requirements are evolving together with these threats, which are becoming inevitable. Thus, there is an ongoing shift in how decision-makers need to holistically look at cybersecurity.

Tackling these risks is becoming increasingly more complicated, and time-consuming, and demands specialised skilled and certified cybersecurity professionals. The cybersecurity skill gap continues to be one of the biggest problems that organisations today are facing as they try to respond to the ever-evolving, sophisticated cyberattacks.

Going into 2023 and beyond, data security solutions will be a top priority. A rise in demand is seen, with data now scattered across various assets. Simultaneously, cyberthreats are not slowing down, and there will be an upsurge in the targeted cyberattacks on end users, endpoints, Internet of Things devices, as well as critical infrastructure, due to the complexities of the digital ecosystem, technology stack, IT and OT convergence, and evolving threat landscape.

Today, most cyberattacks cannot be prevented as they are far too stealthy, targeted, and advanced. Hence, there is a continuous shift from focusing on prevention to recognising the importance of detection and response mechanisms, and this is where GBM Shield comes in, offering a first-of-its-kind programme in the region with an adaptable, holistic, integrated and vendor-agnostic approach.

FOR CISOs

- Get clarity on the guidelines for disclosing data breaches and how the information can be shared.
- Shift focus from prevention to recognising the importance of detection and response mechanisms.
- Go for managed security offerings to protect high-value assets and address critical business-specific risks.

HP

DRIVING THE INDUSTRY FORWARD IN ENDPOINT SECURITY

HP has been investing in research and innovation for over two decades to provide security solutions across user and enterprise levels.

Ertug Ayik, Vice President and Managing Director, MEA, HP.

Cybersecurity spending is expected to increase globally by 13.2% in 2023. However, with the anticipated cut in the budget, organisations are likely to invest in the most pressing cybersecurity needs. Intention and good governance are crucial when it comes to selecting a security partner. One critical thing seen within these constraints is that all investment decisions on infrastructure will be also security decisions.

The threat landscape is increasingly growing with the rise in all forms of attacks, from firmware attacks that take control of an entire system, to destructive attacks designed purely to wreak havoc.

For more than two decades, HP has led the industry forward by investing in research and innovation in endpoint security, having security baked into people's PCs so they can easily prevent, detect and recover from attacks using tools like HP Sure Recover. At the enterprise level, containment technology like HP Sure Click Enterprise help defends against the most common attacks and makes sure that the malware cannot infect anything.

Sophisticated cyberthreats that have the potential to disrupt business operations are major issues that organisations worldwide encounter. A vast majority of those threats can go undetected, or they are detected too late for an organisation to avoid risk. The budget for cybersecurity investment in 2023 won't be unlimited, so it is important to be intentional about where to invest. Compliance is not the only aspect of good governance; it is also about properly managing the company's resources and budget. Knowing which areas expose the company to the most risk will be crucial in understanding the security issues at hand.

In 2023, sophisticated firmware attacks will become more widespread, and the shift to the cloud has made cybercrime easier, cheaper, and more profitable. Traditional security measures have focused on detecting malware to prevent attackers from gaining access to critical systems. Over the last year, we've seen signs of increased development and trading of capabilities, from tools to hack BIOS passwords to rootkits and trojans targeting device BIOS, Basic Input, Output System and UEFI, Unified Extensible Firmware Interface. Increased resiliency or the ability to respond to hackers who've managed to exploit a vulnerability, is key.

Amidst an ever-changing economic climate, manufacturers and channel partners are adapting business strategies as they seek to operate profitably to address supply chain instability and margin pressures. HP is committed to continuing to support its channel, improve supply chain execution, and drive continuous innovation.

HP Amplify Data Insights enhancements give partners immediate access to a rich set of data analytics, each aimed at influencing the customer buying journey and delivering a more satisfying experience. HP has expanded its customer-level insights available through advanced analytics. New automated tools are designed to integrate with partner sales systems, thus simplifying the way data is collected, analysed and delivered to participating partners to convert insights more easily into sales-driven actions.

HP Amplify Impact global expansion is a partner assessment, resource, and training programme that leverages its extensive investments and initiatives across climate change, human rights and digital equity. This allows partners of all types, including resellers, retail, and distribution partners to access the programme regardless of the location.

FOR CISOs

- The budget for cybersecurity investment in 2023 won't be unlimited, hence be intentional about where to invest.
- Focus on the intention and good governance while selecting a security partner for your organisation.
- Identify areas that expose the company to the most risk to fully understand the security issues at hand.

ManageEngine

STAY AHEAD OF REGULATORY AND ATTACK TRENDS

ManageEngine combines threat intelligence, ML tools, and rule-based attack detection techniques to provide effective threat remedies.

Ram Vaidyanathan, IT Security Evangelist, ManageEngine.

The new SEC regulations have made reporting cyber incidents and risk posture critical. While it will impact organisations in several ways, it also means a bigger role for CISOs during the board meetings. They should be prepared to give a detailed analysis of KPIs to demonstrate how their security team functions.

It also means that going ahead customers and investors will factor in the cybersecurity policies of the organisations they deal with and the security maturity of companies will directly impact the top line. It also heightens the need for robust solutions to streamline security efforts and hire personnel with appropriate skills to optimise organisational cybersecurity practices.

ManageEngine invests nearly 50% of its revenue into R&D to provide the best solutions to meet customers' challenges. The company recognises that customers demand a platform rather than a point product. Hence, Log360, the unified SIEM solution, has integrated DLP and CASB capabilities. It combines threat intelligence, Machine Learning, ML-based anomaly detection, and rule-based attack detection techniques to uncover sophisticated attacks, and provides an incident management console for effectively remediating detected threats.

Log360 helps organisations in several ways. It correlates events across the network to discover attack patterns in diverse parts of the network and develops the possible attack kill chain. It also provides unified identity mapping. Security analysts can use this feature to detect cases of credential switching.

The solution also leverages the smart Threshold feature for alerts, utilising the ML capabilities to obtain threshold values for alert profiles automatically. This helps decrease MTTD or mean time to detect security issues. It also utilises the SOAR capabilities, which are pivotal for speedy incident response from one single console leading to a decrease in the meantime to respond or MTTR.

Going ahead, CISOs can expect to face the three key security challenges in 2023. One, they need to build KPIs that can track the risk posture and performance of the Security Operations Centre, SOC. A primary challenge that every CISO faces is aligning security objectives with business goals. They must focus on building successful KPIs that track the risk posture and performance of a SOC team, communicate these to the executive board, and accomplish other vital actions.

With advancements in technologies like AI and ML reshaping the cybersecurity scene, established regulatory standards are being updated and organisations should be prepared to swiftly adopt the latest cybersecurity controls and requirements. Staying ahead of the regulatory standards may prove a big challenge for CISOs in the future.

Hiring, training, and retaining talent is the third challenge area since there is a supply and demand gap in cybersecurity. With a limited number of trained cybersecurity professionals available, hiring and retaining talent is a long-standing challenge CISOs face.

Global and regional trends

Organisations must keep a track of and watch out for top global and regional trends in 2023.

Ransomcloud attacks: Ransomware has entered the cloud environments as well. The attacker sends a phishing email with an attachment that, when downloaded, initiates the installation of ransomware in the user's system. This ransomware presents itself as a harmless pop-up to the user. When clicked, the ransomware disseminates itself, giving the threat actor access to the network.

Supply chain vulnerabilities: There have been cases where attackers enter networks through vulnerabilities or compromised devices present in the network or through access provided to a third-party or partner who is also part of the network or supply chain.

FOR CISOs

- Identify robust solutions to streamline the organisation's security efforts.
- Hire personnel with appropriate skills to optimise organisational cybersecurity practices.
- Keep abreast of the trends and security challenges to swiftly adopt the cybersecurity controls and requirements.
- Focus on building successful KPIs that track the risk posture and performance of a SOC team.

Mimecast

KEEPING COMMUNICATIONS, PEOPLE AND DATA PROTECTED

Organisations need to ensure they have all processes, tools, and systems in place to protect the data they collect and store.

Lara Yousuf, Channel Account Manager, Mimecast.

The recent year has seen an increase in legislation related to personal data protection with the EU's General Data Protection Regulation, GDPR gradually driving global alignment. The UAE announced its Personal Data Protection Law last year and the same will come into effect in Saudi Arabia in March this year. These laws put greater pressure on businesses to protect their customers and other data or risk penalties.

Organisations need to ensure they are compliant and have all the processes, tools, and systems in place to protect and better manage the data they collect and store. By doing so, organisations can build and maintain high levels of trust that can improve their relationship with customers and employees.

The security industry has created a complex web of point products designed to address critical areas of risk. The Mimecast X1 Platform is the company's response to this challenge, helping keep communications, people, and data protected. It encompasses four core innovations.

- Mimecast X1 Precision Detection is engineered to apply the latest advancements in Artificial Intelligence or AI and Machine Learning, ML and enable intelligent detection of emerging and unknown threat types, while layered protection keeps users safe all the way down to the point of risk.
- Mimecast X1 Service Fabric allows customers to grow securely and seamlessly and uncover user insights that can accelerate detection and response, providing the foundation for cloud-delivered security at scale.
- Mimecast X1 Data Analytics provides the foundation for a wide array of services and capabilities, from the discovery and analysis of new threats and accelerated product innovation to rich context for threat researchers and support for cross-correlation of data with systems beyond email. The goal is to make information actionable for customers.
- Mimecast Extensible Security Hooks, MESH, exposes a vast API ecosystem that supports fast, simplified integration of Mimecast with existing third-party security investments.

For years, CISOs have fought to get their boards to take cybersecurity more seriously and they're finally succeeding. There's been a definite shift in thinking with corporate boards finally paying attention to the business risk of cyber threats. Organisations, however, have other financial priorities as well.

The challenge, therefore, will be to get the necessary budget to improve cyber defence. Also, while there is increased awareness at the C-level of the organisation, security teams still need to convince the rest of the organisation that cybersecurity is everybody's responsibility. Consistent and impactful awareness training will be key to changing this mindset.

Traditional attacks such as phishing and ransomware are set to continue, along with more sophisticated social engineering attacks that are increasingly hard to combat. Coupled with the increased availability of complex AI tools, a new wave of attacks is set to plague organisations that are not equipped to quickly detect and deter multifaceted cyberthreats.

Combating ransomware will continue to be a top priority for organisations. Unfortunately, even though the complexity of these attacks has increased, the ransomware defences for most businesses have not evolved to keep pace with it. More than 75% of businesses in the UAE reported experiencing a ransomware attack in the past year, with 44% reporting a loss in revenue due to a ransomware attack.

Threat actors are also likely to take social engineering to the next level, leveraging the growing power of AI voice cloning technology to enhance their impersonation attacks. The use of audio deepfakes will be combined with compromised email and collaboration accounts to improve the hit rate of attacks.

FOR CISOs

- Get the management on board to get the necessary budget to improve cyber defence.
- Put in place automated systems and tools to quickly detect and deter multifaceted cyberthreats.
- Keep updated on trends and evolve security policies to deal with AI voice cloning and audio deepfakes.

NETSCOUT

PROTECTING AGAINST NETWORK VULNERABILITIES

NETSCOUT's solutions and services enable enterprises to take a proactive and comprehensive approach to network security and performance.

Gaurav Mohan, VP, SAARC and Middle East, NETSCOUT

Today's businesses are dealing with increasingly sophisticated cyber-threat tools. Monitoring cyber-threats, correlating intelligence with internal security telemetry and keeping up with adversaries' tactics, techniques, and processes is a difficult task. In reality, bad actors have access to an ever-expanding arsenal of creative and advanced tools, including Artificial Intelligence. Meanwhile, targeted businesses are frequently unaware of the impending risks and lack adequate safeguards to limit the risk.

Innovation is a constant in the realm of cybercrime and criminals are continually innovating and adapting, creating new, more effective attack vectors or simply doubling down on existing, effective techniques. The growth of ransomware and adaptive distributed denial of service or DDoS, in particular, is likely to pose significant risks to global and regional organisations.

The employment of ransomware attacks in conjunction with others such as supply chain attacks is a trend that will continue to expand. Attackers may also continue targeting specific industries or types of businesses with ransomware attacks to maximise their revenues. Hospitals and other healthcare companies, for example, have historically been vulnerable to ransomware attacks because, with lives at stake, they may be more ready to pay a ransom to restore access to crucial systems and data.

Further, adaptive DDoS attacks are expected to grow in popularity. Adversaries conduct significant pre-attack reconnaissance in these operations to identify specific sections of the service delivery chain to target. They are increasingly using botnet nodes and reflectors and amplifiers that are closer to the victim. This reduces the number of barriers that DDoS attack traffic must cross, resulting in fewer possibilities to detect and neutralise the attack. Because of adversary innovation and adapting, defenders must change their way of thinking and, as a result, adapt to the current threat scenario.

No wonder then, CISOs are facing a rapidly expanding attack surface, with an ever-growing number of components including work-from-home users, mobile devices, sanctioned, unsanctioned cloud applications, and Internet of Things or IoT devices. This places greater strain on security teams to understand what is connected to the network, scan for vulnerable assets, monitor network traffic, and fine-tune security measures.

NETSCOUT's latest solutions and services enable enterprises to take a proactive and comprehensive approach to network security and performance. One of the company's latest innovations for businesses is Omnis AIF, an AI-powered solution that enables users to instantly and automatically thwart a significant number of DDoS attacks, streamlining operations and lowering risk exposure.

This approach uses global DDoS attack activity observations to drive local automation and response. As a result, consumers are significantly less vulnerable to DDoS attacks and the possible ramifications for their enterprises.

The company has also recently added nGeniusEDGE Server to the service assurance portfolio. It ensures that enterprises are kept up to date and protected against any potential network vulnerabilities. This all-in-one, plug-and-play solution provides customers with the oversight and information they require to ensure a positive end-user experience, regardless of where staff members conduct their tasks physically.

FOR CISOs

- Change the way of thinking to adapt to current threat scenarios and be cautious of innovative techniques used by adversaries.
- Update security policy to deal with WFH users, mobile devices, sanctioned, unsanctioned cloud applications, and IoT devices.
- Scan everything that gets connected to the network, monitor network traffic, and fine-tune security measures.

Nozomi Networks

AI-POWERING NETWORK VISIBILITY AND SECURITY

Nozomi Networks helps organisations mitigate the challenges of resources while helping track industrial control devices and applications.

As the cybersecurity threat landscape changes, CISOs and their teams will need highly skilled cyber professionals and more advanced cybersecurity solutions to defend against an increasingly sophisticated range of attacks. Cybersecurity professionals need to be able to adapt quickly as new threats emerge and to find new ways to defend their environment while meeting a growing list of government recommendations and requirements.

Expect cyber criminals, hacktivists and nation-state actors to continue to evolve their skills for greater success. This includes hybrid threat tactics like November's Continental ransomware attack launched by hacktivists who used nation-state tactics to cause physical disruption to railroads. Prepare for quantum cybersecurity threats and be on the lookout for malicious AI-driven chatbots.

ChatGPT is a variant of the Generative Pre-trained Transformer, GPT, language model that is specifically designed to generate human-like text based on a given prompt. While ChatGPT can be used in a variety of positive applications, it can also be used in social engineering and phishing attacks. As these systems become more sophisticated, malicious threat actors may add them to their arsenal.

Nozomi Networks recently launched Nozomi Arc, an Operational Technology or OT and Internet of Things, IoT endpoint security sensor that exponentially speeds time to full operational resiliency. Built to automatically deploy across large numbers of sites and devices anywhere an organisation needs visibility, Nozomi Arc adds crucial data and insights about key assets and network endpoints. This data is used to better analyse and deter threats and correlate user activity without straining resources or disrupting mission-critical networks.

Expect cyber criminals, hacktivists and nation-state actors to continue to evolve their skills for greater success

Security professionals are challenged with a lack of security resources and the inability to track industrial control devices and applications. Nozomi Arc addresses both issues while complementing the network-based analysis provided by Nozomi Vantage and Guardian platforms.

The demand for Nozomi Networks' OT and IoT security solutions continues to grow globally. The company continues to grow its channel investments to equip loyal partners with resources and incentives to capitalise on that demand. In addition to supporting high-performing partners with generous profit margins, its ADVantage partner programme includes robust presales support, streamlined processes for deal registration and protection, advanced training and certification, and partner-exclusive demo accounts of the flagship SaaS product Vantage.

Nozomi Networks responded early with AI-powered network visibility and security solutions that integrate and work across IT, OT, edge, and cloud environments. Vantage, and subscription pricing options across the company's entire product portfolio, make it possible for partners to leverage cloud-based industrial cybersecurity for their customers that enables them to scale quickly while minimising complexity and cost.

Alexander Foroozande,
Head Channels MEA, Nozomi Networks.

FOR CISOs

- Cybersecurity professionals must quickly adapt to new threats and find new ways to defend their environment.
- Gear up to meet the growing list of government recommendations and requirements.
- Prepare for quantum cybersecurity threats and be on the lookout for malicious AI-driven chatbots.
- Put in place highly skilled cyber professionals to defend against an increasingly sophisticated range of attacks.

Omnix International

SECURING THE NEXTGEN ENTERPRISE NETWORK

Omnix International enables customers to make their security solutions hybrid cloud-ready for deployment in a variety of environments.

Walid Gomaa, Chief Executive Officer, Omnix International.

The impact of the SEC regulations and global data privacy guidelines is expected to be momentous. Companies around the world are expected to face increasingly stringent requirements for protecting sensitive data, including the identities of their customers and employees.

To deal with the new compliance norms, companies will need to make investments in new technology and change processes to become compliant with the new regulations and framework. These changes are likely to result in greater protection of sensitive information, increased trust in the enterprise, and improved overall security. The challenge is to make sure that these changes will not disrupt current operations.

In 2023, CISOs and security decision-makers are likely to face several ongoing challenges and pain points. One of the primary challenges is the dynamic nature of cyber threats, which means that security teams must be constantly updating their strategies and tools to stay ahead of potential attacks. Another challenge is the increasing complexity of IT environments, which makes it more difficult to identify and mitigate risks across multiple systems and devices.

The trend towards remote work and cloud computing is also putting additional pressure on security teams, as they must find ways to protect sensitive data and systems in these decentralised environments. Lastly, the shortage of skilled cybersecurity professionals is also likely to remain a key pain point for many organisations. These challenges will require CISO and security decision-makers to be more proactive and innovative in their approach.

Going ahead, it is expected that global and regional trends will continue to shape the cybersecurity landscape. Ransomware attacks are likely to remain a major threat, as attackers continue to exploit vulnerabilities in networks and systems. Similarly, identity-based attacks can come in many forms, like phishing, credential stuffing, impersonation and fraud. Impacts can range anywhere from the high costs of recovery to damages from the tarnishing of the business's reputation.

Advanced Persistent Threats or APTs are sophisticated attacks that are carried out by nation-state actors and criminal groups, and they are expected to become more widespread and sophisticated in the year. Organisations can also expect an increase in BOT attacks. Commercial websites are a soft target for BOT attacks which manipulate, defraud, or disrupt a website, application, API, or end-users.

The growing number of connected devices and the increasing use of Internet of Things technology in homes and businesses are likely to lead to a rise in IoT-based attacks. As more organisations adopt cloud computing, the security of cloud infrastructure and data is also going to be a continuous challenge.

Omnix is working on innovative approaches to security solutions that use AI and machine learning algorithms to quickly detect and respond to cyber threats. This helps to minimise the damages caused by breaches and minimise the risk of further attacks. This approach towards automation is aimed at reducing the workload on security teams and improving response times.

The company also helps customers to make their security solutions hybrid cloud-ready so that they can be deployed in a variety of environments. Finally, Omnix offers end-to-end security services and solutions that can provide a comprehensive and coordinated approach to protecting against cyber threats.

It also works with channel partners to find ways to enhance the bottom line. This can be through increased specialisation, channel incentives, training, and joint marketing activities. Omnix has built programmes along with channel partners to enhance current skills and acquire new skills, through joint investments, enabling the company to differentiate itself in the market.

FOR CISOs

- CISO and security decision-makers need to be more proactive and innovative in their approach.
- Explore new ways to protect sensitive data and systems in decentralised environments.
- Deploy end-to-end security solutions that can provide a comprehensive and coordinated approach to protecting against cyber threats.
- Security teams must be constantly updating their strategies and tools to stay ahead of potential attacks.

Proofpoint

MEETING ENTERPRISE SECURITY AND COMPLIANCE NEEDS

Organisations must adopt people-centric solutions to address the security and compliance needs of a cloud-reliant, distributed workforce.

Emile Abou Saleh, Regional Director, MEA, Proofpoint

Proofpoint continues to drive innovation into its product offering, to keep pace with the threat landscape. In the past year, Proofpoint announced a host of people-centric innovations across its entire product line, meeting customer demand for solutions that address the security and compliance needs of today's increasingly cloud-reliant, distributed workforce.

These enhancements empower companies worldwide to stay ahead of a continually evolving threat landscape and better protect their most important asset, their people, from attacks and compliance risks related to email, cloud, data and collaboration tools, wherever they are working.

CISOs and security decision-makers have to contend with even bigger demands in 2023, especially as global tensions escalate, the global economy grows more volatile, and workforce challenges continue. Furthermore, increasingly complex and interconnected digital ecosystems will exacerbate existing concerns and raise new fears about systemic risks, where weaknesses in any one component threaten the strength of the whole.

Proofpoint's research has revealed that email-based threats, such as Business Email Compromise, BEC, ransomware, credential phishing, compromised cloud accounts, and social media hijacking attacks, were common in 2022 as cybercriminals targeted employees to steal credentials, siphon sensitive data, and fraudulently transfer funds. These will continue to be the regional CISO's concerns in 2023.

The global shift to the work-from-anywhere model has increased organisations' reliance on collaboration platforms and cloud technologies to maintain business continuity. In addition, organisations are creating and moving more data than ever before. This in turn creates new forms of security risk for organisations, making it challenging to both understand when data is at risk and implement the proper control to mitigate that risk.

Increasingly complex and interconnected digital ecosystems will exacerbate existing concerns and raise new fears about systemic risks

With the evaporation of the traditional network perimeter, the old way of protecting data does not work. There is a need to up the game and adopt Data Loss Prevention tools and insider risk solutions to protect the modern edge, including endpoint, cloud apps, email, and the web.

FOR CISOs

- Deploy tools to understand when data is at risk and implement proper control to mitigate it.
- Adopt DLP and insider risk solutions to protect the modern edge, including endpoint, cloud apps, email, and the web.
- Stay ahead of evolving threat landscape to protect people from cyberattacks and compliance risks.

Sophos

MAKING MANAGED DETECTION AND RESPONSE HAPPEN

Sophisticated cyberattacks can be difficult to deal with, but MDR solutions can help quickly collate attack traits and respond.

Harish Chib, Vice President, MEA, Sophos.

The new SEC regulations have put notable security requirements on public companies, especially around incident reporting. While there are benefits to this, including the share of threat intelligence, the regulations put new stress on organisations to maintain security protocols. One strategic solution is the use of Managed Detection and Response or MDR services. It can help organisations comply with SEC regulations by detecting security incidents earlier, collating gathered threat intelligence and analysis, and providing a proper incident response.

Sophos MDR is a fully-managed threat hunting, detection, and response service that provides a dedicated 24X7 security team to rapidly identify and neutralise complex threats. Their innovative service fuses Machine Learning with human threat analysis for an evolved, innovative approach to proactive security protection.

The service combines Sophos' top-rated endpoint protection and data-driven XDR with a world-class team of experts to counteract and prevent threats. Overall, Sophos MDR protects around 15,000 organisations and is available to businesses of all sizes as a turn-key solution, hybrid solution, or both.

The cybercrime-as-a-service industry has reached a new level of commercialisation and commodification, removing entry barriers for anyone interested in committing cybercrime. This has potentially increased the volume of attacks. It also means that CISOs and security decision-makers need to plan and develop cybersecurity approaches that will help them prioritise indicators and signals of attack, so they can respond as quickly and efficiently as possible.

One way to do this is through MDR solutions that automatically collate similar attack traits appearing across an entire network. The Sophos MDR team uses this unique technology to determine connections between attacks, which enables them to better prioritise and action immediate response.

Going ahead in 2023, businesses must be wary of new versions of cyber threats and malware. Stolen credentials, for example, are damaging because they allow attackers to impersonate legitimate users on the network. To detect these attackers, the best defence is what is called Eyes on Glass or threat hunters who look for anomalies indicating a stealth attacker is hiding in plain sight.

At Sophos, the threat hunters are looking for these anomalies and other indicators of compromise 24X7. Attackers can strike at any time, often during off hours or on weekends, so it is important to constantly monitor the network. If organisations lack the staff to do so, they should work with a security partner with the resources to protect, detect and respond around the clock.

With the launch of an updated partner programme, Sophos partners across levels can do deal registration for MDR opportunities, irrespective of the size of the company. Partners are also offered a new MDR sales certification. This, ultimately, enhances margins and the customer contract value. It is important that partners need to look at the organisation's security as a whole.

By starting with MDR, they can easily assess weaker areas that need attention, such as a stronger perimeter and endpoint protection, so attacks are not getting into the network in the first place. Sophos provides partners with all of the tools they need to secure their customers, from services to endpoint and network solutions.

FOR CISOs

- Develop cybersecurity approaches that prioritise indicators and signals of attack for swift and efficient threat response.
- Get Eyes on Glass or threat hunters who can look for anomalies indicating a stealth attacker is hiding in plain sight.
- Constantly monitor the network because attackers can strike at any time, often during off hours or on weekends.

Vectra AI

ADD INTELLIGENCE TO ENTERPRISE CYBER DEFENCE

Get AI-driven threat detection and response platform for hybrid and multi-cloud enterprises to stay ahead of modern cloud-based cyberattacks.

As enterprises shift to hybrid and multi-cloud environments embracing digital identities, digital supply chains, and ecosystems they are faced with higher security risks and compliance issues. It also means that security and compliance leaders, architects and analysts have to continuously deal with increasing attack surfaces, vulnerabilities, and exploits.

There are more evasive attacker methods, system intrusion, and infiltration. They also have to deal with a growing number of tools, alerts, rules, tuning, noise, and triage. All these are leading to more burnout, more turnover and ever-increasing skills and talent gaps.

One can call this the vicious spiral of more. The more organisations shift applications and data to the cloud, the bigger the spiral becomes and the faster it accelerates, creating more challenges for the security operations centre or SOC teams. Amid the spiral of more, threat detection and response have become more complex and less effective.

Today, nearly every security category, vendor and tool include some measure of threat detection, from vulnerability and posture management tools to endpoint, network, cloud, application and data protection tools. And all of them claim accurate threat detection. There are simply too many disparate, siloed tools creating too much detection noise for a SOC analyst to manage. To make matters worse, attackers thrive on noise because it makes it easier for them to infiltrate an organisation, blend in and progress unseen.

One big trend we see is that Multifactor Authentication or MFA continues to be a prime target for attackers. With identity attacks on the rise, in 2023 attackers will continue to take advantage of vulnerable MFA methods. As companies continue to roll out MFA, attackers will continue to take advantage, either by flooding end-users with requests to brute-force their way in, or by skilled phishing campaigns.

End-users will be the ones directly targeted by attackers. This means not just organisations, but also consumers will need to be more aware than ever of the risks to their digital identities. Meanwhile, organisations must ensure they have tools in place to detect suspicious login activity and stop it in its tracks.

Vectra erases the unknowns with the best Artificial Intelligence or AI-driven threat detection and response platform for hybrid and multi-cloud enterprises, delivering the attack coverage, signal clarity and intelligent control that security teams need to get ahead and stay ahead of modern cloud-based cyber-attacks.

Attack coverage: Vectra provides attack coverage across four of an organisation's five attack surfaces, including Cloud, SaaS, Identity, and Networks. It helps monitor attacker TTPs throughout the entire cyber kill chain and across hybrid and multi-cloud attack vectors.

Signal clarity: With patented Attack Signal Intelligence, the Vectra solution comes armed with AI-driven prioritisation. This enables security analysts to focus on the most urgent threats to the organisation like hunting, investigating, and stopping attacks from becoming breaches.

Intelligent control: This includes integrated investigations, automated workflows, and targeted response actions and enables organisations to optimise security investments in tools, processes and playbooks to boost SOC efficiency and effectiveness.

Vectra also lays equal emphasis on channel enablement programmes, which are announced periodically through its dedicated partner portal. These have expanded during the past 24 months to include several new incentive schemes. It has also enhanced the innovative online demo system, which helps partners quickly familiarise themselves with new platform functions and features, enhancing their presales capabilities. Additionally, The company has also onboarded key personnel in METNA, in the sales, engineering, marketing, and channel functions.

Taj El-khayat, Area VP, South EMEA, Vectra AI.

FOR CISOs

- Plug MFA vulnerabilities to reduce identity attacks, including brute-force attacks and skilled phishing campaigns.
- Ensure the organisation has appropriate tools in place to detect suspicious login activity and stop it in its tracks.
- Include integrated investigations and targeted response actions to optimise security investments.

DATA INTELLIGENCE PARTNER FOR GLOBAL ENTERPRISES

With 6,000+ cybersecurity specialists worldwide, Atos supports clients through their digital transformation in compliance with regulations.

Charles PIRON, Global Channel Sales Director, Cybersecurity Products, Atos.

Data is now at the heart of the digital economy. While artificial intelligence and machine learning can help unleash its value, data also needs to be secured, computed, and processed at the right location. With key expertise in high-performance computing, edge computing, cybersecurity and critical systems, Atos is a trusted data intelligence partner for large organisations around the world.

With wide-ranging technology expertise and more than 6,000 cybersecurity specialists worldwide, Atos supports clients throughout their digital transformation in compliance with regulations.

Atos is known in the market as a service company with strong expertise in compute and cybersecurity. Every interaction with a customer starts with a set of dedicated experts who understand customer's industry and their IT challenges. Each region of the world requires a specific sales and delivery strategy. In Middle-East, Atos incentivizes and motivates channel partners to propose its solutions to their key customers.

Partnerships

Atos differentiates from the competition by owning some of the products involved in its solution. Atos develops, manufactures, and maintains cutting-edge cybersecurity and compute products that combine HPC, Edge servers, Mission critical systems, Hardware Security Modules, Data Encryption, Access Management and Digital Identities. These offers are known on the market under the brand of Bull, IDnomic, Cryptovision, Evidian IAM and Trustway.

Atos is also working closely through strong partnerships to provide customer with an end-to-end security and compute capabilities delivering consulting, hardware, software, and services to its customers.

Market focus

In a world where cyberattacks are increasing in volume and sophistication, below are the key industries where cybersecurity can be provided to meet their specific challenges:

> Atos incentivizes and motivates channel partners to propose its solutions to their key customers

Financial
Services address cybersecurity challenges as part of banks and insurance digital business transformation. The use cases we are implementing are key management, tokenisation, access management to trading rooms or employees' authentications, transaction encryption, standard and advanced digital signature.

Public sector
Atos protects critical services and infrastructure with end-to-end digital security:

- Securing public administration digital transformation
- Securing citizen services
- Securing smart infrastructure and critical services

Energy and utilities
Atos combines trust and compliance for the digitalisation of production. Atos cybersecurity is for example involved in protecting the smart-meters and grid systems making sure that our customer can focus on their business.

Telecom
The convergence of new technologies such as edge, cloud, OpenRAN and 5G creates major new opportunities for telecommunications companies to meet the challenges of competitive markets, pressure on costs, and rising expectations of customers.

Atos provides telecom security for 4G,5G network and resiliency with security orchestrator. Cybersecurity assets used in this industry are strong authentication, digital identities and data encryption at core.

Solutions

Atos with its cybersecurity division, acts as a trusted partner to secure the digital world in many domains:

Trusted Digital Identities
Identities need to be protected to avoid breaches. You need to ensure the integrity of identities and access control of your company. The Atos Trusted Digital Identities solution enables you to provide secure and convenient access to critical resources for business users and devices, while meeting compliance demands

Industrial and IoT Security
With the number of connected objects growing exponentially, both IoT security and OT security are growing concerns that need to be addressed with a security by design approach

Data Protection and Governance
The journey to cloud, IoT and OT security or digital workplace can only be started once we know the maturity level of the organisation. One of the other key concerns while adopting those moves is the protection of sensitive data.

Hybrid Cloud Security
Moving to the cloud is no longer a question of "if," but "how." How to move securely to the cloud and how to keep control of data (including sensitive data) while benefiting from the flexibility of the cloud

Advanced Detection and Response
Supervision and orchestration are key features needed for a 360° view of what's happening in the organisation – on-premises and in the cloud. Atos Managed Detection and Response brings multi-vector threat detection and full-service response at speed, leveraging 16 SOCs.

Atos believes that innovative, collaborative end-to-end cybersecurity is a strong asset and a competitive differentiator for any organisation. In addition to the thousands of experts and technologies deployed around the world, Atos cybersecurity experts participate in numerous working groups and are members of several leading cybersecurity communities.

The content has been provided by the partner.

Layale Hachem,
Senior Solutions Engineer,
BeyondTrust.

PRIVILEGED ACCESS, PRODUCTIVITY AND SHADOW IT

Robust PAM delivers granular control of applications across Windows, Mac, Unix, Linux, network devices, without hindering end-user productivity.

Behind the UAE's escalating battle with threat actors is a number of factors. One of them is the increased incidence of shadow IT, which is the use of technology hardware and software outside the sphere of influence of the IT department. It is not hard to see why.

When working from home, the opportunity is there, unfettered by watchful eyes. And sometimes, in order to get things done, it is quicker to bypass IT, which takes care of motive.

Nowadays, even entire unvetted clouds make their way into the technology stack without the awareness of the CIO and their team. Pressure on IT to relax controls, just so that operations remain slick, leads to further problems. File-sharing, storage, and collaboration applications used without due oversight can facilitate incursions and data leaks. And personal email accounts can introduce similar vulnerabilities if used to send attachments to a work inbox.

Even shadow IoT, when added to a corporate Wi-Fi network without IT's knowledge, can wreak havoc.

> "Shadow IT has real-world costs associated with it, not only potential breaches and their resultant downtime, but scalability issues"

Shadow IT starts to become dangerous when off-the-grid digital assets get in the way of vulnerability management, patch management, configuration management, identity management, through rogue user accounts, privileged access management, because it abandons the principle of least privilege, or log management, because unauthorised tools do not have access to security logs.

Any one of these issues give a leg up to threat actors, allowing them to drop malware payloads and establish backdoors for future incursions. They also place undue strain on helpdesks because of device compatibility issues, and put the organisation on a collision course with regulators, should an incident occur because of shadow IT.

A hindrance

Shadow IT has real-world costs associated with it — not only potential breaches and their resultant downtime, but scalability issues. Shadow IT can prevent agile growth of the technology stack and yield ongoing hidden costs such as when payments continue to be made from corporate or personal accounts when a shadow IT user leaves the organisation.

So how can IT teams shine a light into the murky world of shadow IT and sift out incidences for action? One of the best ways is through careful implementation of privileged access management, PAM.

Visibility of assets

PAM platforms are made for network visibility because they are capable of the automatic discovery of any device that accesses the environment. PAM can also discover which users have access to which privileged credentials. PAM tools support onboarding, privilege management, monitoring, and auditing.

Least privilege

The principle of least privilege grants access to each digital asset only for those accounts, human and machine that need it to perform an authorised business task, and even then, only for as long as access is needed. Robust PAM delivers granular control of applications across Windows, Mac, Unix, Linux, and network devices, and it does so without hindering end-user productivity.

Remote access

RDP, VPN, and legacy remote-desktop tools are short on granular access-management controls, and yet they are vulnerable to session hijacking. In the age of remote work, PAM solutions take VPNs out of the equation to provide secure privileged access for vendors, employees, service desks, and infrastructure. PAM applies least privilege and audit controls over remote access, thereby reducing the risk of unauthorised remote access via shadow IT.

Beyond PAM

PAM alone will not get the job done, however. Many best practices that supplement or enhance PAM will be necessary if we are to eliminate the threats that stem from shadow IT. It may seem obvious, but a good starting point is a simple acknowledgement that shadow IT is present.

Next on the list is the establishment of an adequate management policy, followed by a culture change in which IT learns to say yes more often — yes to new projects, yes to new ideas, yes to change in general. The default not possible must be banished from the IT department's phrasebook. Over time, this may make allies of the very employees who would otherwise engage in shadow IT.

There are also methods that can be deployed to discover shadow IT and classify its risk to the business. For example, if the shadow component carries unencrypted PII, personally identifiable information or unpatched vulnerabilities, this would constitute a greater risk than a machine or application that did not.

Bubbles begone

If it sounds like the medicine for shadow IT is a blend of tools, PAM and a new culture of collaboration between IT and everyone else, that is because, largely, it is. Accepting you have a problem such as shadow IT is the first step, but fixing the problem requires some work, some hard decisions, some will, and some good faith.

We should be clear that the eradication of shadow IT really amounts to the eradication of the risk it poses. In some instances, given the right culture, a tool may not be procured that may have been procured under a different culture. Understanding from IT on why shadow assets spring up and understanding from end users on their potential threat will create a middle ground from which to work.

CLOUD SECURITY GETTING BETTER ALL THE TIME

Cloud providers are in a virtuous circle of security improvements providing a foundation for security professionals to build their cloud security programmes.

Frank Kim, Fellow and Lead for the Cloud Security and Security Leadership curricula at SANS Institute and CISO-in-Residence, YL Ventures.

Rapid innovation is driving organisations to adopt cloud services as critical infrastructure. Cloud acceleration has become a boardroom issue, with non-technical leaders often being vocal proponents of cloud as the route to achieving wide-ranging business objectives. However, cloud innovation can introduce security risks if rushed.

Cloud security providers are constantly improving their security offerings and capabilities. As a result, businesses may be tempted to rely on these cloud-native security services. However, the most effective approaches rely on enterprise security teams building expertise and capabilities in-house to build a proactive security programme.

Security professionals need time and resources to ensure appropriate protection for the business. Here's how they can help their business forge a solid foundation for secure and effective cloud acceleration.

Getting started

Organisations are moving critical assets, data, and processes to the cloud, making it an obvious target for attackers. As such, cybercriminals are growing savvier about how to gain initial entry, compromise accounts, escalate privileges, take advantage of misconfiguration, and much more.

Security teams need to use threat modelling to keep tabs on cloud attacks and impacts. Understanding adversary tactics and techniques in cloud attack scenarios make it possible to detect breaches before data or assets are exposed and prevent lasting damage.

Cloud threat modelling requires the consideration of a range of factors: adversaries, attack techniques, outcomes and risks, and countermeasures. It is also highly strategic.

First, define what to model threats for, such as an entire system or a component. Second, look at threats – what can go wrong? An account hijack? A vulnerable package exploited in a container image? Third, look at mitigations and controls that can reduce or eliminate risk. Finally, validate that the analysis conducted has been thorough and reasonable.

Demystifying attackers' strategies

Many organisations today are leveraging the MITRE ATT&CK model to help frame threats. Understanding the typical phases of attack can

feed into building a proactive cloud threat model. For example, initial access is gained by exploiting public-facing applications, exploiting trusted relationships, or discovering valid accounts in cloud environments.

Persistence is where an attacker takes steps to ensure they can return at will. At the same time, privilege escalation is a common goal to access valid accounts or to manipulate role assignments. Alongside this, attackers will often use access to seek out other resources that may be vulnerable. Following this, collection and exfiltration see data moved to a location under the attacker's control.

Cloud threat modelling across the attacker's entire lifecycle will unveil potential vulnerabilities and establish proactive security mitigations.

Next, let's look at three core pillars for mitigation.

Pillar #1 – Identity and Access

Identity and access management defines who needs access to what and controls the entire life cycle of user and access management across resources. Mature organisations will centralise identity and access wherever possible. Another benefit of a centralised identity approach is reduced operational overhead.

One significant cloud-driven shift in identity management is the advent of machine identities versus traditional human identities. Machine identities include services accounts for systems like cloud VMs, cloud functions, and containers and help mitigate the risk of other technical accounts used for programmatic actions and deployments.

> Cloud threat modelling across the attacker's entire lifecycle will unveil potential vulnerabilities and establish proactive security mitigations

Pillar #2 Data Security

A sound data security strategy for the cloud is a fundamental requirement. Undoubtedly, one of the most important security controls for data protection in the cloud is encryption. Cloud providers have the capability to implement encryption at scale reasonably easily. For some organisations, this automatic encryption will prove sufficient. In many other cases, though, data protection will need to be more specific.

Another key factor is secrets management. Managing sensitive secrets, including encryption keys, API keys, passwords, and other credentials has proven immensely challenging for most organizations. Data Loss Prevention is also essential, with many organisations turning to DLP tools and services, which can be notoriously difficult to implement and maintain.

There are ways of managing all of these challenging factors within the cloud, but ideally where threat modelling has revealed where risk can be best mitigated.

Pillar #3 Visibility

The third critical pillar of cloud security is visibility, with an emphasis on logging, event management, and automation through guardrails. Visibility goes beyond traditional system and network visibility but must cover applications, systems, networking, and their configurations in the cloud. This concept also applies to control plane visibility and visibility of the cloud environment itself. In addition to extensive logging of all activity within the cloud, several new services are available to continuously monitor cloud accounts and infrastructure for best practices configuration and security controls status.

To achieve network visibility, tools such as network firewalls and intrusion detection and prevention can be used alongside the collection of network flow data. Cloud-native access controls and monitoring capabilities can also monitor and track network events and behaviours.

Take action.

Cloud security is getting better all the time. The key advantage of the public cloud is that cloud providers are in a virtuous circle of security improvements. This provides a strong foundation for security professionals to build their cloud security programs.

However, as cloud services grow, security teams must use more advanced controls and develop more dynamic processes for evaluating security in the cloud to ensure success. This means conducting regular threat modelling exercises and focusing on three primary mitigation categories - identity and access management, data security, and visibility – to provide a dynamic foundation for cloud security.

GLOBAL CISO FORUM

PRESENTS

11 MAY QATAR | 18 MAY KSA | 25 MAY UAE

GCC SECURITY SYMPOSIUM AND CISO AWARDS 2023

7TH EDITION

SEC_RITY IS NOT COMPLETE WITHOUT U!

BROUGHT TO YOU BY

GEC MEDIA GROUP

OFFICIAL MEDIA PARTNERS

Enterprise CHANNELS MEA

BUSINESS TRANSFORMATION

CYBER SENTINELS