

SPECIAL SUPPLEMENT BY

Enterprise
CHANNELS **MEA**

VOLUME 06 | ISSUE 2 | **AUGUST 2024**

CYBER SENTINELS

NASSER AL NEYADI

Head of Information Security
Operations, Digital Security,
and Smart Services
Ministry of Interior UAE

CHAMPIONING CYBERSECURITY

UAE Ministry of Interior leads the way in cybersecurity
and digital innovation

Lexar



WORLD'S FASTEST
Memory Solution



Cloud was initially pitched as inherently more secure than on-premises systems. While this may be true to a great extent due to service providers investing in advanced security controls, recent reports suggest that 80 percent of companies have experienced at least one cloud security incident in the past year. Additionally, it is estimated that 45 percent of data breaches are now cloud-based.



JEEVAN THANKAPPAN
jeevan@gcemediagroup.com

The pandemic-induced digital transformation frenzy has pushed many organizations to adopt cloud technologies, often without giving adequate attention to security considerations. The shift to the cloud has introduced new types of threats and challenges, making it essential for enterprises to adopt new tools and practices to mitigate these risks.

Common cloud security challenges include lack of visibility, access management, multi-tenancy issues, and misconfigurations. One of the ways to bolster cybersecurity is to follow the best practices prescribed by

the National Institute of Standards and Technology (NIST), which has outlined essential steps that organizations can use to self-assess their security preparedness.

Additionally, an emerging technology that supports the implementation of NIST's cybersecurity framework is Cloud Security Posture Management (CSPM). CSPM solutions are specifically designed to address misconfigurations, a prevalent issue in many cloud environments.

In this issue of Cyber Sentinels, we've collaborated with leading CISOs and industry experts to delve into this crucial topic. Our aim is to provide insights that will help your organization take the necessary steps to secure your cloud environments. It's essential to remember that cloud security is a shared responsibility—don't rely solely on your service provider.

CYBER SENTINELS

PUBLISHER

TUSHAR SAHOO
TUSHAR@GECMEDIAGROUP.COM

CO-FOUNDER & CEO

RONAK SAMANTARAY
RONAK@GECMEDIAGROUP.COM

GLOBAL HEAD, CONTENT AND STRATEGIC ALLIANCES

ANUSHREE DIXIT
ANUSHREE@GECMEDIAGROUP.COM

MANAGING EDITOR

JEEVAN THANKAPPAN
JEEVAN@GECMEDIAGROUP.COM

ASSISTANT EDITOR

SEHRISH TARIQ
SEHRISH@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

SENIOR DESIGNER

SHADAB KHAN

GRAPHIC DESIGNER

JITESH KUMAR
SEJAL SHUKLA

DESIGNED BY



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



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
©copyright 2013 Accent Infomedia. All rights reserved.
while the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

CONTENTS

AUGUST 2024

EVENT
18-27



CISO OPINION CORNER



09

FAISAL KHAN
DWTC



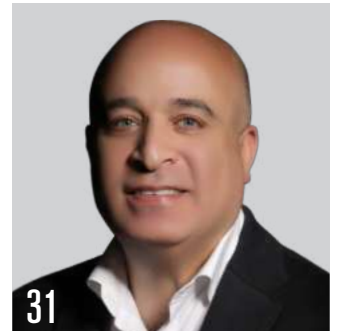
16

RICHARD SOROSINA
Qualys



28

EZZELDIN HUSSEIN
SentinelOne



31

MAHER JADALLAH
Tenable



34

TAREK KUZBARI
Picus



37

RICARDO FERREIRA
Fortinet



39

CHRISTOPHER HILLS,
BeyondTrust



42

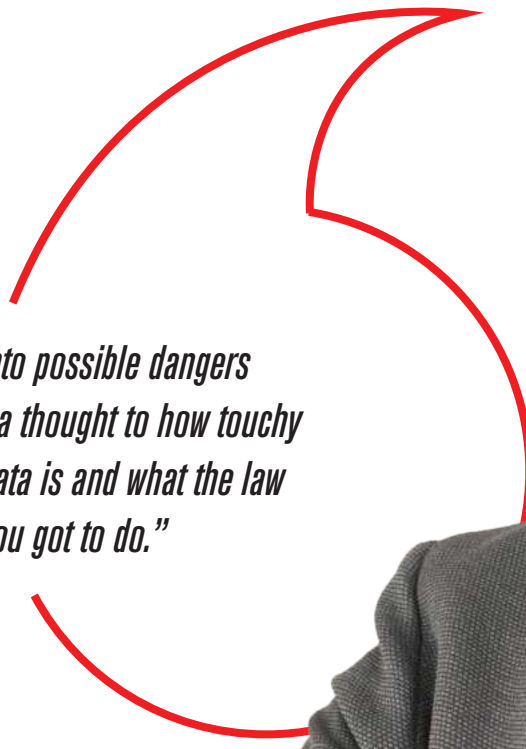
MATTHEW PRINCE
Cloudflare

SECURING CLOUD ENVIRONMENTS

? What are the biggest challenges you face in securing cloud environments?

I've encountered several challenges in ensuring the security of cloud environments. While moving to cloud services offers numerous benefits, it also introduces unique issues that require careful management. One of the primary hurdles is maintaining visibility and control, as the dispersed nature of cloud services makes it difficult to have a comprehensive view of data and resources. Implementing real-time monitoring and management tools is essential.

Additionally, data security and privacy are paramount, necessitating strong encryption, strict access controls, and regular audits to safeguard sensitive information. The cloud's inherent risks mean that governance and adherence to privacy regulations are critical. Moreover, robust identity and access management (IAM) practices are vital, involving rigorous authentication



“Dig into possible dangers giving a thought to how touchy your data is and what the law says you got to do.”

MANOHARAN MUDALIAR
CISO,
Truebell Group of Companies





processes and careful management of access rights, along with ongoing reviews to prevent misconfigurations that could lead to unauthorized access.

Compliance with various regional regulations adds another layer of complexity, making it essential to stay compliant to avoid legal issues and protect sensitive data. Understanding the shared responsibility model between the cloud provider and the customer is also crucial, requiring clear communication to ensure that all security aspects are covered. Finally, the rapid pace of technological change in the cloud sector poses a constant challenge, necessitating continuous learning to stay ahead of emerging threats and leverage the latest security features.

? How do you assess and manage the risks associated with cloud adoption?

I have a comprehensive and dynamic approach to conducting risk assessments and mitigating the dangers associated with cloud migration. This involves first identifying and cataloging all assets being moved to the

cloud, assessing potential threats based on data sensitivity and legal obligations, and continually monitoring for vulnerabilities. Risks are then prioritized by evaluating their potential impact on operations, reputation, and compliance, allowing for the most critical threats to be addressed first. To reduce these risks, I have implemented robust security measures such as encryption, access controls, and intrusion detection, while clearly defining security responsibilities with cloud service providers and maintaining constant vigilance through continuous monitoring. Compliance with relevant laws and internal governance is ensured through well-defined data handling policies. Evaluating cloud partners for their security capabilities and contractual safeguards is essential, along with educating the team on cloud security best practices and staying updated on emerging threats. Preparedness for incidents is also a priority, with a tested response plan and business continuity strategies in place to minimize downtime and data loss. Lastly, I emphasize continuous improvement by reviewing incidents and refining strategies while keeping abreast of the latest advancements in

cloud security and evolving threats.

? What measures do you have in place to protect sensitive data stored in the cloud?

Safeguarding sensitive data in the cloud is a top priority for us, and we employ a multi-layered approach to ensure its protection. We encrypt sensitive data both at rest and in transit, using strong algorithms that make it unreadable without decryption keys, while access controls, including role-based access control (RBAC) and multi-factor authentication (MFA), minimize the risk of unauthorized access.

Additionally, data masking and anonymization techniques protect confidentiality during testing or analytics, and we ensure that personally identifiable information (PII) is removed from datasets. Continuous monitoring and comprehensive logging are employed to detect suspicious behavior and provide an audit trail for forensic analysis.

Data loss prevention (DLP) solutions are implemented to monitor and control the movement of sensitive data, preventing

unauthorized transfers. Regular audits, compliance checks, and third-party assessments are conducted to ensure adherence to data protection regulations and standards.

We also maintain regular encrypted backups and robust disaster recovery plans to ensure business continuity in case of incidents. Vendor management includes thorough due diligence and contractual safeguards with cloud providers to ensure they meet our security and compliance standards. Our commitment to data security is unwavering, and we continuously enhance our measures to protect against unauthorized access, data loss, and breaches, adapting to evolving threats.

? What is your approach to incident response in a cloud environment?

We've got a thorough plan to deal with incidents in cloud settings. Here's how we handle it:

1. Preparation:

- Incident Response Plan: We keep an up-to-date plan that spells out who does what and how to handle incidents made to fit our cloud setup.
- Team Training and Drills: Our incident response team (IRT) often practices and runs through made-up scenarios to stay sharp.
- Toolset Readiness: We use special tools to watch, spot, and react to issues. We test and update these tools.

2. Detection and Analysis:

- Non-Stop Watching: We keep an eye out all the time to catch odd activities and system quirks right away.
- Automated Alerts and Logs: Systems send alerts about fishy activities, and detailed logging helps us analyze everything.
- Threat Intelligence: We plug in threat intelligence to keep up with new threats and link them to incidents we spot.

3. Containment, Eradication, and Recovery:

- Immediate Containment: We focus on cutting off threats to stop more damage.
- Eradication: We work on getting rid of the main problem, like malware, and securing systems that got compromised.
- Recovery: We bring systems and data back to normal, make sure everything's intact, and watch for any lingering issues.

4. Post-Incident Activities:

- Post-Incident Review: Look into the response, spot lessons, and check the

incident timeline and how well it worked.

- Documentation and Reporting: Write down incidents in full and get reports ready for key people.
- Ongoing Improvement: Apply what we've learned to update the response plan, rules, and training.

5. Working Together with Cloud Service Providers:

- Teaming Up with CSPs: Keep good ties with CSPs to share resources and know-how when incidents happen.

? How do you evaluate the security posture of your cloud service providers?

Evaluating the security posture of our cloud service providers (CSPs) is crucial for securing our cloud infrastructure. Our approach includes the following key steps:

1. Due Diligence and Research:

- Security Certifications and Compliance: Review CSP compliance with standards like ISO 27001, SOC 2, PCI DSS, and GDPR.
- Publicly Available Information: Examine security whitepapers, audit reports, and incident histories for transparency and track record.

2. Security and Compliance Assessments:

- Security Controls Evaluation: Assess CSP security controls in data encryption, access management, network security, and incident response.
- Compliance with Legal and Regulatory Requirements: Ensure CSP adherence to relevant regulations and industry-specific standards.

3. Third-Party Audits and Certifications:

- Independent Audits: Review third-party audits and certifications for independent assessment of security practices.
- Penetration Testing and Vulnerability Assessments: Request evidence of regular testing and assessments to identify security weaknesses.

4. Service-Level Agreements (SLAs) and Contracts:

- Security Provisions in SLAs: Carefully review clauses related to data protection, incident response, and breach notifications.
- Contractual Safeguards: Negotiate safeguards for data ownership, deletion, and audit rights.

5. Continuous Monitoring and Reporting:

- Monitoring Tools and Dashboards: Use CSP-provided tools for real-time security

status tracking.

- Regular Security Reviews: Conduct regular reviews and meetings to discuss security performance and improvements.

6. Incident Response and Support:

- Incident Response Capabilities: Evaluate CSP's ability to manage incidents and ensure they have a robust plan and team.
- Support and Escalation Procedures: Understand CSP's support tiers, response times, and technical support availability.

7. Data Governance and Control:

- Data Access and Ownership: Ensure clear policies for data access and ownership, maintaining control and encryption capabilities.
- Data Residency and Privacy: Assess data residency and privacy policies for compliance with regulations and internal policies.

8. Vendor Risk Management:

- Risk Assessment Framework: Include CSPs in a broader vendor risk management framework, with regular risk assessments.
- Exit Strategy and Data Portability: Plan for smooth transitions if changing providers, ensuring data portability and secure transfer.

? How are you addressing the security implications of multi-cloud and hybrid cloud environments?

Handling safety issues in multi-cloud and hybrid cloud setups involves implementing a unified safety plan that ensures consistent security rules across all cloud environments to minimize configuration errors and gaps. Centralized control tools are used to oversee and enforce policies, ensuring compliance from a single point of management. User and access control (UAC) is streamlined through shared user management, providing secure and seamless access across platforms with single sign-on and multi-factor authentication, while role-based access control (RBAC) assigns necessary permissions to reduce the risk of unauthorized access and insider threats. Data security is reinforced with unified encryption standards for both stored and in-transit data, alongside data classification and segmentation to apply appropriate controls based on sensitivity and regulatory requirements. Network security is enhanced through secure connectivity using VPNs, secure gateways, and specialized interconnects, with micro-segmentation to isolate workloads and limit the spread of



attacks.

Visibility and monitoring are achieved through tools like logging, intrusion detection systems (IDS), and security information and event management (SIEM) systems, complemented by machine learning and data analytics to detect anomalies and address potential threats.

Collaboration with cloud service providers (CSPs) is crucial, maintaining strong ties to leverage their expertise for updates, best practices, and incident management, while also considering vendor risks across multi-cloud and hybrid environments to mitigate potential risks from multiple providers.

? What role do AI and machine learning play in your cloud security strategy?

Recognizing the transformative potential of AI and ML in enhancing cloud security, our organization is actively exploring these technologies through a careful and phased approach. Currently, we are evaluating AI and ML solutions for threat detection, anomaly detection, and predictive analytics, with a focus on their maturity, stability, and accuracy to avoid false positives. Potential applications include using AI and ML to detect unusual patterns in cloud environments, enhance threat intelligence by analyzing global data for proactive defense, and automate incident response tasks such as isolating compromised systems or adjusting firewall rules.

Future adoption considerations involve ensuring seamless integration with existing security infrastructure, addressing data privacy and ethical concerns, and developing the necessary skills within our security team. Our long-term vision includes a gradual implementation strategy, beginning with pilot projects to test the effectiveness and reliability of these technologies, along with continuous monitoring and improvement to maximize benefits and minimize risks. While AI and ML are currently in limited use, we acknowledge their significant potential and are committed to a thoughtful, controlled adoption as these technologies mature and demonstrate reliability.


? What advice would you give to organizations just beginning their cloud security journey?

Starting a cloud security journey requires establishing a strong foundation that balances innovation with security. It's essential to understand the Shared Responsibility Model by clarifying the roles and responsibilities between your organization and the cloud service provider (CSP) to ensure effective security measures. Conducting a comprehensive risk assessment helps identify and prioritize potential threats and vulnerabilities, considering data sensitivity and compliance requirements. Implementing strong identity and access management (IAM) by enforcing the principle of least privilege, utilizing

multi-factor authentication (MFA), and regularly reviewing access controls is crucial. Encryption and data protection should be leveraged by encrypting sensitive data both at rest and in transit, with data classification guiding appropriate security controls. Developing a robust incident response plan that is regularly updated and includes collaboration with CSPs for clear incident management is vital. Continuous monitoring and visibility can be achieved by implementing monitoring tools and integrating them with Security Information and Event Management (SIEM) systems for centralized analysis. Compliance and governance must be ensured by aligning security measures with regulatory requirements and establishing governance policies for data management and security controls.

Education and training for your team on cloud security best practices, including specialized training for IT and security staff, are important. Starting with small pilot projects allows for testing security strategies in controlled environments before full deployment, with an iterative approach to gradually expanding cloud services while refining security measures. Finally, evaluating and choosing trusted CSPs with strong security and compliance reputations, along with negotiating Service Level Agreements (SLAs) that include clear terms for security, compliance, and incident response, are critical steps in your cloud security journey. ➡

STRENGTHENING CLOUD SECURITY WITH AI AND MACHINE LEARNING

A portrait of Faissal Khan, a man with a dark beard and mustache, wearing a dark pinstripe suit jacket over a light blue button-down shirt. He is looking directly at the camera with a slight smile. A red curved line graphic is positioned to the left of his face, framing a quote.

“Understand your data and classify it by sensitivity in-line with ensuring compliance with relevant local regulations and laws.”

FAISAL KHAN

Head of Information
Security and Compliance,
DWTC

? What are the biggest challenges you face in securing cloud environments?

We understand that the challenges faced are many and require a combination of robust security practices. There is no one solution in the market that can make our lives easy as Security Professionals.

These challenges vary from the selection of the right tools, technologies, practices, and a thorough understanding of cloud security principles and responsibilities. This challenge however becomes even more difficult, when there are so many CSPs to engage and onboard with for our business priorities.

? How do you assess and manage the risks associated with cloud adoption?

Assessing and managing the risks associated with cloud adoption involves a comprehensive approach that considers technical, operational, and organizational factors. These risks are largely related to data governance and compliance in line with

Govt regulatory requirements and national laws. When evaluating the cloud model, our first approach is to ensure that the benefit we get from the cloud service is aligned with the business objectives and strategy also ensuring the security measures which should be as per our expected levels. We do also weigh the advantages and disadvantages of cloud adoption when it comes to handling sensitive government data which should always be protected through the CSP's security controls. A key factor is to also ensure that in the event of an incident or disaster, what will be the SLAs that would have a direct impact on objectives as defined under our organizational goals.

? What measures do you have in place to protect sensitive data stored in the cloud?

We use a combination of best practices to evaluate a CSP before onboarding them in line with the highlighted risks above. Over and above, we use a combination of tools to monitor and protect our cloud solutions such as MFA, CASB, DLP, IAM, Attack Surface, and Data Encryption while as practices to name a few, we make sure that we perform

Regular Access and Configuration Reviews, Third-Party Risk Audits and Vulnerability Assessments. These measures provide us with significant assurance and satisfaction in reducing risks.

? What is your approach to incident response in a cloud environment?

We have playbooks created for all possible scenarios on containment, mitigation, recovery, and post-incident activities as part of our incident response strategy. This is both for our on-premises and on-cloud services and infrastructure. We also rely on Continuous Monitoring and Alerting support using our SOC Services and also on our CSPs to provide us with their MDR & XDR services to give us multiple layers of security when it comes to prevention and recovery of services. This methodology gives us assurance and readiness to react to an incident if it takes place.

? How do you evaluate the security posture of your cloud service providers?

We use a Cloud Security Checklist covering the necessary security controls and best





practices to evaluate and assess a CSP for our cloud environment needs. These assessments include ensuring onboarding checks such as CSP's local presence in the country for data residency, secure and robust infrastructure, seamless interfacing, visibility and control over our data, business continuity, and specially the rapid changes in technology creating increased security gaps which are of prime concern.

? How are you addressing the security implications of multi-cloud and hybrid-cloud environments?

The growing challenges of failures and downtimes as experienced with CSPs these days don't come to us as a surprise. Attackers being aware of organizations now hosted in the cloud makes them a perfect target to sabotage their services. For this specific reasonings, it is always the best approach for any organization to distribute their workloads across a multi-cloud environment. This not only guarantees resilience but also ensures that not all their services would be impacted in an event a threat is posed upon them. However, it has to

be noted that with the IAAS model, a multi-cloud approach can work effectively whereas not all other PAAS, SAAS might not be available leaving room for a hybrid approach. Nevertheless, approaching any model needs a thorough assessment considering the alignment with the organizational.

? What role do AI and machine learning play in your cloud security strategy?

AI and machine learning (ML) play a significant role in enhancing cloud security strategies by providing advanced capabilities for threat detection, response, and overall security management. We are no different when it comes to recognizing the fact that in the current digital era, reliance on AI/ML will and will in-turn yield greater benefits for our business model, as being the biggest and largest events and exhibitions organization in the region.

By leveraging AI and machine learning, we have been able to enhance our cloud security strategy with more accurate threat detection, faster incident response, improved compliance, and overall better risk management. These

practices help us to align and protect our brand and reputation.

? What advice would you give to organizations just beginning their cloud security journey?

For organizations embarking on their cloud security journey, they need to focus on several key essential criteria. These steps will help build a solid foundation for securing the desired cloud infrastructure.

- Understand your data and classify it by sensitivity in-line with ensuring compliance with relevant local regulations and laws.
- Choose reputable cloud service providers with strong security practices.
- Implement robust access controls and encryption for data protection.
- Regularly monitor and audit your cloud environment for unusual activity.
- Develop and test an incident response plan specific to cloud environments.
- Continuously update your security measures to address emerging threats.
- Train employees on cloud security best practices. ➡

AT THE FOREFRONT OF CHAMPIONING CYBERSECURITY

In this exclusive interview, First Lieutenant Nasser Al Neyadi, Head of Information Security Operations, Digital Security, and Smart Services at the UAE Ministry of Interior, discusses how to navigate the intersection of cybersecurity and digital innovation.

**NASSER AL NEYADI**

Head of Information Security Operations, Digital Security, and Smart Services
Ministry of Interior UAE

? How has digital transformation impacted your organization's security strategy?

Digital transformation has fundamentally reshaped our organization's security strategy. With the rapid adoption of new technologies and digital processes, we've had to become more agile and proactive in our approach. This means integrating security measures from the very beginning of our digital projects, rather than treating them as an afterthought. We've also placed a stronger emphasis on continuous monitoring and threat intelligence to stay ahead of potential threats in this dynamic landscape. The shift to digital also necessitates a broader understanding of potential vulnerabilities, including those introduced by third-party vendors and supply chains. As a result, we have developed more comprehensive risk management practices and fostered a culture of security awareness across all levels of the organization.

? What role does cybersecurity play in enabling digital innovation within your organization?

Cybersecurity is a critical enabler of digital innovation within our organization. By ensuring robust security measures are in place, we can confidently pursue new technologies and digital initiatives without compromising our data or systems. Effective cybersecurity practices help build trust with our stakeholders, ensuring that innovation can proceed smoothly and securely. It also allows us to take calculated risks, knowing that we have the necessary safeguards to protect our assets. This trust extends to our customers, partners, and regulatory bodies, who can see that we prioritize their security and privacy. Furthermore, by embedding security into our innovation processes, we can streamline compliance with industry standards and regulations, which can often be a barrier to the adoption of new technologies.

? What strategies do you use to secure cloud-native applications?

Securing cloud-native applications requires a multi-faceted approach. We prioritize identity and access management (IAM) to ensure only authorized users have access to our cloud resources, use encryption to protect sensitive data both in transit and at rest, and employ continuous monitoring with

advanced tools to detect suspicious activities and potential breaches. Additionally, we leverage automation for security policies and compliance checks to maintain consistency and reduce human error and integrate DevSecOps practices to identify and mitigate vulnerabilities early in the development lifecycle. We also adopt micro-segmentation to isolate workloads and limit the impact of potential breaches. Regular security audits and penetration testing are conducted to ensure that our defenses remain robust against evolving threats. By adopting a zero-trust model, we further ensure that trust is continuously verified, minimizing the risk of unauthorized access.

? What role do you see for security in the broader context of business transformation and innovation?

Security plays a foundational role in business transformation and innovation. As organizations evolve and adopt new technologies, security must be embedded into every layer of the process. This ensures that innovations are not only effective but also resilient against cyber threats. A strong security posture enables businesses to explore new opportunities confidently, knowing they can protect their assets and maintain customer trust. In the broader context, security facilitates regulatory compliance, which is essential for operating in various industries and markets. By integrating security with business strategies, we can create a competitive advantage, demonstrating our commitment to protecting sensitive information and maintaining operational integrity. This holistic approach to security also helps in building a robust reputation, which is crucial for long-term success in today's digital economy.

? How do you balance the need for security with the need for speed and agility in digital projects?

Balancing security with speed and agility is challenging but achievable with the right approach. We integrate security into the development process through DevSecOps, allowing us to catch issues early without slowing down progress. Automation plays a crucial role in streamlining workflows by providing automated security testing and compliance checks. Additionally, we focus



on risk management by identifying and prioritizing the most critical areas, ensuring that security measures do not hinder innovation. Collaboration between security and development teams is also essential to achieve common goals efficiently. By adopting agile methodologies, we can iterate quickly while embedding security checks within each sprint cycle. Continuous integration and continuous delivery (CI/CD) pipelines further enhance our ability to deliver secure software rapidly. This approach not only accelerates the development process but also ensures that security remains an integral part of our digital projects, maintaining a balance between protection and progress.

? How do you see the role of the CISO evolving with advancements in digital technologies?

The role of the CISO is evolving from being a purely technical leader to a strategic business partner. As digital technologies advance, CISOs need to understand the broader business implications of security decisions. They must work closely with other executives

to align security initiatives with business goals, drive innovation, and manage risks effectively. CISOs will also need to stay abreast of emerging technologies like AI and machine learning to leverage them for enhanced security measures. This evolution includes fostering a culture of security awareness and ensuring that security strategies support business agility. As digital transformation accelerates, the CISO's role will expand to include responsibilities such as data privacy, compliance, and even digital ethics. They will need to be adept at communicating the value of security investments to stakeholders and demonstrating how these investments enable business growth. The ability to foresee and mitigate risks associated with new technologies will be crucial, positioning the CISO as a key driver of innovation and business resilience.

? What future trends in digital transformation, AI, and cloud do you think will have the biggest impact on security?

Several trends are poised to significantly

impact security: AI and machine learning will enhance threat detection and response capabilities but also introduce new risks that need to be managed. Zero Trust Architecture is shifting security models towards continuous trust verification. Cloud security is becoming critical as more organizations adopt multi-cloud and hybrid environments. The proliferation of IoT devices introduces new attack vectors, and quantum computing, though still emerging, could revolutionize cryptography and data protection, requiring new security approaches. These trends will drive the need for continuous innovation in security strategies to protect against evolving threats. Additionally, the integration of AI in security operations centers (SOCs) will automate routine tasks and improve the accuracy of threat detection, allowing security teams to focus on more complex issues. The rise of edge computing will also necessitate new security frameworks to protect data and processes closer to where they are generated. Overall, staying ahead of these trends will require a proactive approach to security, with a focus on adaptability and resilience. ➔



AMPLIFY YOUR VOICE
WITH US AND EXPLORE
OUR SERVICES.



DESIGN
SERVICES



PHOTOGRAPHY &
VIDEOGRAPHY



2D & 3D
ANIMATION



TELE-
CALLING



EVENT
MANAGEMENT



MEDIA
BUYING



DIGITAL
MARKETING



CORPORATE
GIFTS



SOCIAL
MEDIA



BRAND
ACTIVATION



BOOTH
BUILDING



CONTENT
GENERATION

www.brandvoize.com

REDEFINING SECURITY

Richard Sorosina, Chief Technical Security Officer EMEA and APAC, Qualys, on how to deal with unmanaged devices and security

Over the past three years, the position of zero trust and access control has become more and more important to CISOs. According to the annual Leadership Perspective Survey published by Gartner peer community company, Evanta, in 2024, the category of User Access, IAM and Zero Trust is now the number one functional priority for CISOs, taking over from cloud security. However, while many CISOs want to adopt a zero trust mindset and embrace better security for their operations, getting to this goal is much harder than they imagine.

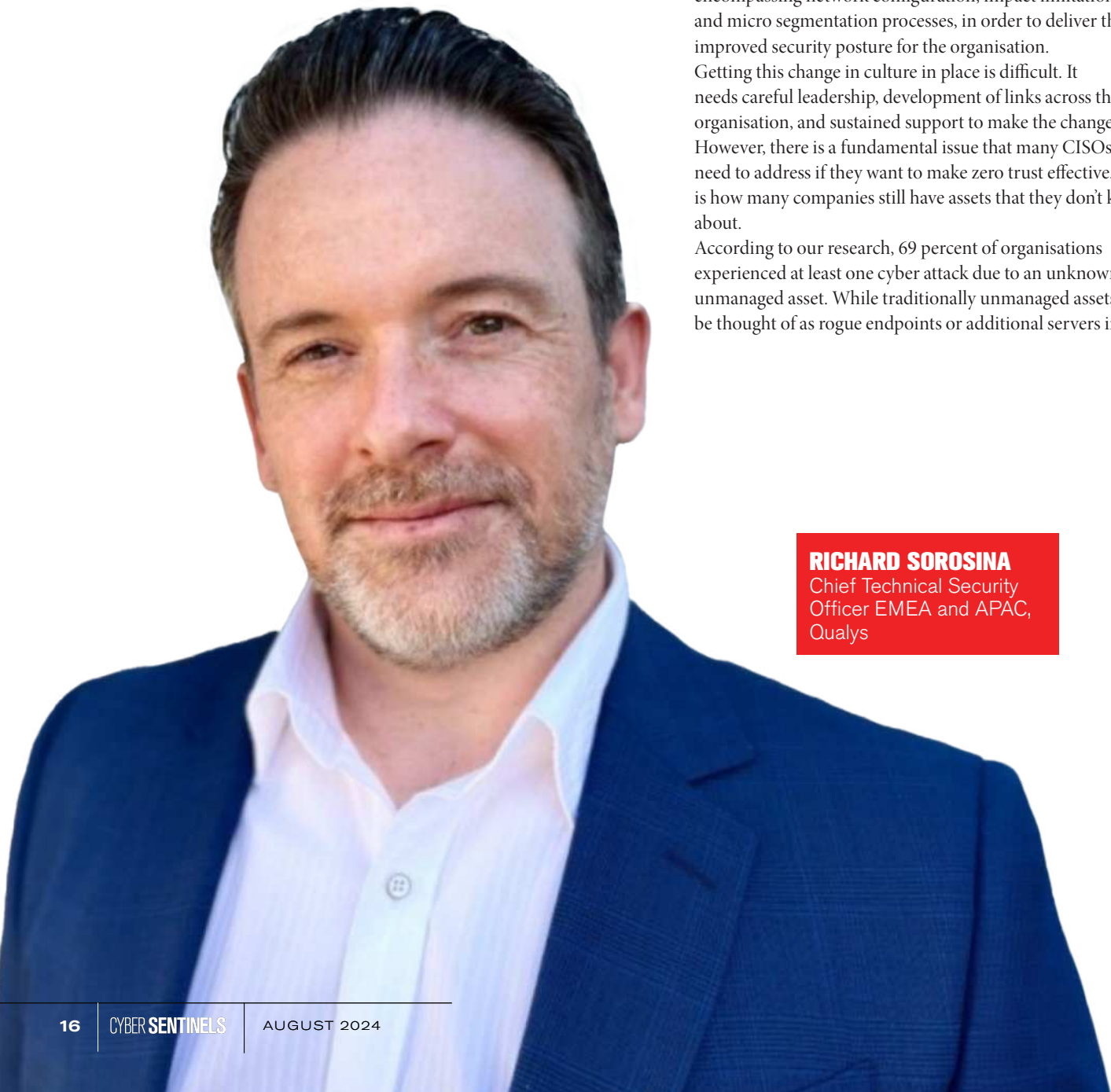
Zero trust and proactive security

CISOs want to implement zero trust because it reduces the likelihood of a breach and the potential impact of any breach that does occur. It also makes it easier to take a proactive risk management approach across the organisation. As part of this, it focuses on unmanaged devices. The Zero Trust Security Architecture model states that no assets (inside or outside the perimeter) should be automatically trusted.

The issue around zero trust is that it is not a technology project. Instead, implementing zero trust involves adopting a comprehensive philosophy across all security operations, encompassing network configuration, impact limitation and micro segmentation processes, in order to deliver that improved security posture for the organisation.

Getting this change in culture in place is difficult. It needs careful leadership, development of links across the organisation, and sustained support to make the change stick. However, there is a fundamental issue that many CISOs still need to address if they want to make zero trust effective. That is how many companies still have assets that they don't know about.

According to our research, 69 percent of organisations experienced at least one cyber attack due to an unknown or unmanaged asset. While traditionally unmanaged assets might be thought of as rogue endpoints or additional servers in the



RICHARD SOROSINA

Chief Technical Security
Officer EMEA and APAC,
Qualys



data centre, today these assets can include a wide variety of IT services, including software installed, cloud-based workloads, user accounts that have not been properly managed, and connected Internet of Things (IoT) devices too. Each of these assets can either get onto the corporate network or connect to it, and then represent a potential route for an attack.

In our work with companies, we found that CISOs had to add on average 34 percent more assets to their asset lists. This represents a huge additional overhead for companies around their IT, increasing management costs and potential risks for the future, if not addressed.

How to solve the problem

To address these issues and make zero trust a reality, we first have to admit where the problems are. Some of these may surprise you.

The first issue is whether we recognise that there is a problem around IT asset management at all. After all, while you can't secure what you don't know about, how many of us put this at the top of our to do lists? If your asset list is incomplete, then you are not able to make accurate decisions on what to prioritise across cloud workloads, containers, IoT systems, mobile devices, remote endpoints, and Operational Technology (OT) deployments. In turn, this can affect all

your assumptions on risk modelling and how secure you really are. We may end up being massively over-confident about how much risk the business is exposed to.

The second issue we have to admit is that we may not address asset management as a critical competency. Instead, it is often delegated or passed around the team, and treated as a chore. It also relies on multiple teams to carry out the work involved. Without executive attention, it is hard to keep any asset list up to date, current and accurate. When it is treated as a critical task, then it will get the investment and concentration needed. Alongside senior level support, we have to recognise that existing enterprise software tools cannot illuminate every platform.

While we might have an accurate view of the cloud, say, we might not have that same level of accuracy and insight for IoT devices. Using any one tool to get the information we need is not reliable enough when there are so many platforms in place. Instead, we have to collaborate and use different methods to get all the data that we need, then organise it effectively. This includes blending a range of different technologies, from active and passive scanning techniques and security agents to API-based discovery tools.

This combination will establish a comprehensive inventory of all your IT assets and keep it up to date in real time. This record should allow your team to automatically

distinguish between trusted and untrusted assets and make decisions on how to handle those assets effectively. In turn, this makes it easier to apply zero-trust principles across all your devices.

Applying a risk-based approach

Once you can see all your assets, you can make more accurate and informed decisions around risk. With companies having a third more IT assets on average than they expect, that category will include a range of different assets that will vary from inconsequential and forgotten devices through to critical applications that suffered from what Douglas Adams called the "Somebody Else's Problem Field" issue.

Knowing about those assets is the first step to improving security across a diverse device landscape. Based on this information, you can set out a zero trust strategy and then concentrate your resources on those devices, applications and workloads that are critical to the business. This approach reduces the potential impact of any breach, shrinks the potential attack surface and makes risk management programs more effective. Unmanaged devices represent a significant risk to security programs, but getting insight into all the devices that might enter your network is not impossible. It just needs prioritisation. ➡



Tech Titans Unite

World CIO 200 Summit In Indonesia Catalyzes Digital Innovation

The recent World CIO 200 Summit, held in Indonesia marked a significant milestone in the global IT landscape, bringing together thought leaders, innovators, and industry experts to share insights, discuss challenges, and explore opportunities in the ever-evolving digital world. The event commenced with a warm welcome note from Jennefer Lor-

raine Mendoza, Project Lead Manager at GEC Media Group. Jennefer set the tone for the summit by highlighting the critical role of technology in driving innovation and efficiency in today's business environment.

Following the welcome address, the stage was graced by Hendy Harianto, Group CIO of Meratus Group, and Ichwan Peryana, Co-Founder



& Director of Pinjam Modal (PT Finansial Integrasi Teknologi), for the Ambassador Keynote session. Their keynote speeches underscored the importance of leadership and strategic vision in navigating the complexities of digital transformation.

The first panel discussion, moderated by Benny Jioe, Head of Digital Transformation at PT Zurich Asuransi Indonesia Tbk, focused on "Agility and Adaptability." This session emphasized the need for organizations to be agile and adaptable in the face of evolving cultural dynamics and market conditions. Panelists Andri Hidayat, Digital Service Transformation & IT Director at PT. Prodia Widyahusada Tbk, Kevin Kane, Chief Technology Officer at Bank Amar Indonesia Tbk, Setiaji Setiaji, Chief of Digital Transfor-

mation Office at the Ministry of Health of the Republic of Indonesia, and Yusron Anas, Chief Information Officer at Home Credit Indonesia, shared their experiences and strategies for fostering innovation and staying ahead of the curve.

The summit also featured a compelling vendor keynote, offering valuable insights into the latest technological advancements and their applications in various industries.

In the session on "Collaborative Innovation," Prabaharan (Praba) Gopalan, Chief Information Officer at Indika Energy Group, moderated a discussion with panelists Sudarto Unsurlany, Head of Digitalization at PT. Petrosea Tbk, Edwin Adiwinata, Chief Information Officer at PT Sepatu Bata Tbk, Sigit Triwibowo, Head of IT and Digital – Chief

Technology and Digital at IKEA Indonesia, Indra S. Adillah, Head of ICT at Indonesia AirAsia, and Hendy Harianto, Group CIO of Meratus Group. This discussion highlighted the power of collaboration in driving technological innovation and transforming business operations.

The World CIO 200 Summit successfully provided a platform for IT leaders to exchange knowledge, network, and explore collaborative opportunities. The insights and strategies shared during the event will undoubtedly contribute to the continued growth and evolution of the IT industry. The summit concluded on a high note, with participants leaving inspired and equipped with actionable ideas to drive digital transformation in their respective organizations.



World CIO 200 Summit in Malaysia Sparks Malaysia's Digital Future

Global CIO Forum proudly announces the successful conclusion of the The Works CIO 200 Summit held in Kuala Lumpur, Malaysia. The event brought together a distinguished gathering of over 200 CIOs, IT leaders, and industry experts to discuss the evolving landscape of digital transformation and the pivotal role of technology in shaping the future.

The summit commenced with a warm welcome note by Anushree Dixit,

Global Head of GEC Media Group, who set an inspiring tone for the day. Anushree emphasized the importance of collaboration and innovation in driving technological advancements and achieving organizational goals.

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab, Chief Executive Officer of Cybersecurity Malaysia, delivered the Country Inaugural Keynote. Dato' Ts. Dr. Haji Amirudin highlighted the critical role of cybersecurity in



today's digital era and shared valuable insights on building robust cyber defenses to protect organizational assets and data.

Ts. Saiful Bakhtiar Osman, Head of IT – Shared Services at PNB Commercial Sdn. Berhad, followed with the Ambassador Keynote. Ts. Saiful Bakhtiar emphasized the significance of strategic IT leadership in fostering innovation and driving business growth.

The summit featured a dynamic panel discussion on "Creating a Unified Vision: Stress the importance of aligning diverse stakeholders around a shared vision for transformation, transcending cultural differences to create a unified sense of purpose and direction." Moderated by Mr. Akmal Nizam, Director – IT at Lembaga Tabung Angkatan Tentera (Malaysia Army

Funds Board), the panel included:

- Melvin Foong Mun Hoe, CIO of GDeX Berhad
- Vijayaananth Arumugam, Head of IT Infra & Data Science at SD Guthrie Research Berhad
- Ts. Ahmad Kamal Hasan Basri, Head of Group IT at MARA Corporation

The session provided valuable perspectives on aligning diverse stakeholders and creating a cohesive vision for digital transformation.

Suja Raghav, Territory Sales Manager at Kissflow, presented an insightful session on KISSFLOW, showcasing innovative solutions for streamlining business processes and enhancing organizational efficiency.

The final session, "Technology as a Catalyst,"

was moderated by Dr. Peter Leong, Business Director at MYCIO Services. The panel, comprising:

- Zainol Zainuddin, CTO of IPay88
- Vijaykumar Dayinde, CIO of Malaysia Airports
- CH Nghoh, Director Corporate Information Centre at Help University

examined how technology serves as a powerful catalyst for transformation, facilitating communication, collaboration, and the seamless integration of processes across borders.

The Global CIO 200 Summit concluded on a high note, leaving attendees inspired and equipped with valuable knowledge and strategies to drive digital transformation within their organizations.



World CIO 200 Summit Mumbai Edition Celebrates Success with Industry Leaders and Key Insights

The World CIO 200 Summit, held on August 10, 2024, brought together industry leaders, IT experts, and influential CIOs for an evening of insightful discussions, knowledge sharing, and transformative ideas. Hosted by GEC Media Group, the event proved to be a resounding success, offering a platform for thought leaders to explore the latest trends and innovations shaping the future of technology.

Opening Session: The summit commenced with a warm welcome note from Anushree Dixit, Global Head, GEC media Group, setting the tone for an evening of engaging discussions and networking.

Panel Discussions: The event featured several thought-provoking panel discussions:

- **Creating a Unified Vision:** Moderated by Amit Saxena, VP-IT (CIO) at Millennium Semiconductors India Pvt Ltd, Pune, the panel included Sabyasachi Chakraborty Thakur (CIO, Parksons Packaging Limited), Mahesh Toshniwal (Group Head of IT Operations, Jindal Steel and Power), Ajay Awale (Head IT, Aquapharm Chemicals Pvt Ltd), and Rajesh Kulkarni (DGM - IT, Piaggio Vehicles Pvt Ltd). The discussion emphasized the importance of aligning stakeholders for successful transformation.
- **Advancing Organizational Resilience:** Rajeev Dutt, General Manager MEA & APAC at Swiss GRC, provided valuable insights on how enterprises can build and maintain resilience in today's dynamic



environment.

- **Agility and Adaptability:** Led by Pradipta Patro, Head IT & Global CISO at RPG Group, the panel explored how CIOs are enabling rapid innovation. Panelists included Shrenik Kothari (Regional IT Infra Head, Gestamp Automotive India Pvt Ltd), Prashant Kurhade (DGM IT, Suhana Group), Rahul Mergu (Vice President IT, MarketsandMarkets Research Pvt Ltd), and Vivek Sakarde (Chief Data and Analytics Officer, Leading Bank).
- **Gen AI – Use Cases, Infrastructure Readiness, and Adaptability:** Moderated by Jeevan Thankappan, the panel included Satish Mahajan (Sr General Manager IT, VFS Global Services Pvt Ltd), Shabbir Badra (VP & Head IT, Apraava Energy), Rajeev Khade (Chief Digital, Blue Star Limited), Lalit Trivedi (CIO & CISO

Global, FlexM Global Pte. Ltd), and Shashi Mohan Singh (Chief Digital Officer, Reliance Retail Ltd). The discussion focused on the future of AI in business applications.

Technical Sessions:

- **Unified Cybersecurity Platform Approach:** Satyen Jain, Technical Director at LTS, highlighted the necessity for a unified approach to cybersecurity for comprehensive protection.
- **Trends and Technologies Shaping Networks:** Gokul Sorari, Manager of Systems Engineering at CommScope India Pvt Ltd, discussed current and future trends in network technology.
- **Application Security:** Lakshmi Das, COO and Co-Founder of Prophaze, alongside Diptesh Saha, CISO & Practice Head at Accel Cybersecurity, shared their expertise

on the critical aspects of application security.

- **Trends and Technologies Shaping Networks:** Gokul Sorari, Manager of Systems Engineering at CommScope India Pvt Ltd, discussed current and future trends in network technology.
- **Application Security:** Lakshmi Das, COO and Co-Founder of Prophaze, alongside Diptesh Saha, CISO & Practice Head at Accel Cybersecurity, shared their expertise on the critical aspects of application security.

The World CIO 200 Summit provided an invaluable opportunity for networking, learning, and collaboration among top IT professionals. The event underscored the importance of innovation, agility, and strategic vision in navigating the complexities of today's technological landscape.



Innovative Ideas and Collaboration Shine at The World CIO 200 Summit in the Philippines

The World CIO 200 Summit in the Philippines concluded successfully, bringing together a dynamic assembly of the nation's top IT leaders and innovators. This prestigious event, held in Manila, provided a unique platform for CIOs and industry experts to discuss, deliberate, and devise strategies to navigate the ever-evolving landscape of information technology.

The summit commenced with Jennefer Lorraine Mendoza, Project Lead Manager at GEC Media Group, delivering an insightful welcome note at 4:00 pm. Her address set the tone for the day's discussions,

emphasizing the critical role of CIOs in driving digital transformation.

Philip A. Varilla, Assistant Secretary for Infostructure Management at the Department of Information and Communications Technology, followed with the Country Inaugural Keynote, highlighting the government's initiatives and vision for the country's digital future.

Arlene Romasanta, Director of Knowledge and Information Systems Service at the Department of Environment and Natural Resources, presented the Country Ambassador Keynote. Her speech underscored the importance of knowledge management and environmental sustainability



in IT practices.

The first panel discussion, titled "Unleash the Might: Creating a Unified Vision and Stressing on the Importance of Aligning Diverse Stakeholders Around a Shared Vision for Transformation", was moderated by Arlene Romasanta. Esteemed panelists included:

- Sheridan Leroy Laroza, Senior Director of Information Technology at Thermo Fisher Scientific
- Norman Carcellar, Chief Information Officer at Unioil
- Dennis Omila, Executive Vice President and Chief Transformation Officer at Union Bank of the Philippines
- Lito Villanueva, Executive Vice President and Chief Innovations and Inclusion Officer at Rizal Commercial Banking Corporation (RCBC)

This discussion delved into the strategies for

aligning diverse stakeholders around a unified vision for digital transformation, emphasizing collaboration and shared objectives.

The second panel discussion, "Agility and Adaptability: How CIOs are Enabling Organizations to Pivot and Innovate Rapidly to Stay Ahead of the Curve", was moderated by Robert Sanchez Paguia, Chief of the International Cooperation on Cybercrime Division and Data Protection Officer at the Cybercrime Investigation and Coordinating Center. The panel featured:

- Alex Ustaris, CTO at PHINMA Education Holdings Inc
- Albert Silva, Director of the Information and Communications Technology Center at San Beda University
- Julius Caesar Principe, Chief Information and Transformation Officer at FWD Life Insurance

- Dr. Mary Joy Abueg, Vice President at the National ICT Confederation of the Philippines

- Francis Chiu, First Vice President IT at BDO Unibank

This session focused on how CIOs are driving agility and innovation within their organizations, enabling them to quickly adapt to changes and stay competitive in a fast-paced digital world.

The World CIO 200 Summit in the Philippines successfully provided an enriching experience for all participants, fostering collaboration, innovation, and strategic thinking among the nation's top IT leaders. The event highlighted the pivotal role of CIOs in shaping the digital future and reinforced the importance of agility and adaptability in today's rapidly changing technological landscape.



Global CIO Forum SEA Summit Leads the Charge in Singapore

The Global CIO Forum recently orchestrated a trailblazing event in Singapore, heralding a transformative era in digital innovation and synergy among IT leaders in Southeast Asia. This momentous summit united some of the region's most visionary minds in technology and business, fostering a dynamic exchange of insights, strategic deliberations, and the unveiling of avant-garde solutions for the digital frontier.

Welcome Note – Charting the Course

The event commenced with a welcome note from Malavika Shanker, President SEA, GEC Media Group, who set the tone for the evening by highlighting the importance of the Global CIO Forum's mission in

Southeast Asia. She emphasized the need for continuous learning, collaboration, and adaptation in the rapidly evolving digital landscape.

Navigating the Global CIO Forum Journey

Anushree Dixit, Global Head, GEC Media Group, took the stage to present “Charting the Path: Navigating the Global CIO Forum Journey.” She shared the forum's journey from its inception, spreading across 50 countries, and highlighted the exciting plans for the 2024 edition in South Africa. Anushree's presentation underscored the forum's commitment to fostering global collaboration and knowledge sharing among CIOs.



Journey Thus Far: Global CIO Forum & RosettaNet GS1 Digital Standards Consortium

Manoj Saxena, Chairman of RosettaNet GS1 Singapore, provided an insightful overview of the partnership between the Global CIO Forum and the RosettaNet GS1 Digital Standards Consortium. He discussed the importance of digital standards in driving seamless integration and interoperability in the global digital economy.

Fireside Chat with Guest of Honour

A fireside chat with Mr. Loh Sin Yong, Director of Trade Trust (IMDA), served as a highlight of the evening. Mr. Loh shared his perspectives on the role of digital trust in international trade and the importance of secure and transparent digital transactions.

His insights resonated with the audience, emphasizing the critical role of trust in the digital age.

Unleash the Might: Creating a Unified Vision

The panel discussion titled “Unleash the Might: Creating a Unified Vision” focused on the importance of aligning diverse stakeholders around a shared vision for transformation. Moderated by Nicole Tretwer, VP Business Development Integrated Logistics, the panel featured esteemed speakers Clara Lee, Chief of Data Science Practice at NUS-ISS; Mayda Lim, Managing Director, Group Technology & Operations at OCBC; Natalie Que, Chief Information, Digital and Data Officer – Southeast Asia and North Asia at Kenvue; and Juliana Chua, Sr. Director & Head at EssilorLuxottica.

The panelists shared their experiences and strategies for fostering collaboration and driving innovation within their organizations.

Kissflow Presentation

Suja Raghav, Territory Sales Manager at Kissflow, delivered an engaging presentation on the power of digital transformation in streamlining business processes and enhancing operational efficiency. Suja highlighted how Kissflow’s solutions empower organizations to adapt to the digital age with agility and precision.

The Magic of AI to Enhance Customer Journey

The final session of the evening, “The Magic of AI to Enhance Customer Journey,” explored how artificial intelligence can revolutionize customer experiences.

GUARDING THE CLOUD

Ezzeldin Hussein, Regional Senior Director, Solution Engineering, META, SentinelOne, on how to secure the cloud.

? Why is cloud security critical for businesses today?

Cloud security is crucial for businesses today due to the rapid adoption of cloud technologies and the increased reliance on digital infrastructure. As organizations migrate to cloud environments for

scalability, cost-efficiency, and flexibility, they face heightened risks of data breaches, cyberattacks, and compliance issues. The cloud introduces unique security challenges, such as managing diverse workloads, securing sensitive data across various platforms, and ensuring regulatory compliance.

Effective cloud security protects against threats by securing data, applications, and services hosted in the cloud, safeguarding intellectual property and customer information. It also helps maintain business continuity by preventing disruptions and ensuring reliable access to critical systems. With often dynamic and complex cloud environments, robust cloud security measures are essential for mitigating risks, achieving regulatory compliance, and maintaining trust with customers and stakeholders.

? What are the most common threats to cloud security?

Common threats to cloud security include data breaches, where unauthorized access exposes sensitive information, and misconfigurations, which result in security gaps due to improperly set permissions or exposed storage. Insecure APIs pose risks by allowing exploitations through weak interfaces, while insider threats from employees or contractors can lead to data leaks or intentional breaches.

Additionally, Distributed Denial of Service (DDoS) attacks overwhelm cloud resources, disrupting the service. Account hijacking involves the compromise of credentials to gain unauthorized



EZZELDIN HUSSEIN

Regional Senior Director,
Solution Engineering, META,
SentinelOne

access and data loss results from accidental or malicious deletion. Another threat is that insecure interfaces and APIs can be exploited to breach systems, while compliance violations occur when regulatory requirements are not met, leading to legal issues. Furthermore, supply chain attacks target third-party services or software, potentially compromising the entire cloud environment. Addressing these threats requires comprehensive security measures and vigilant monitoring.

? How do these threats differ from those faced by traditional on-premises systems?

In cloud environments, threats often arise from the shared nature of resources and the dynamic, remote management of infrastructure. This introduces risks such as insecure APIs and misconfigurations less prevalent in on-premises systems. Cloud systems also face unique risks from multi-tenancy, where vulnerabilities in one tenant's environment can potentially impact others. Additionally, cloud environments often involve complex, distributed architectures and third-party services, increasing the attack surface compared to more contained on-premises systems.

On the other hand, traditional on-premises systems primarily deal with physical security threats, such as unauthorized physical access and hardware vulnerabilities. These require direct management of network and system security. In contrast, cloud environments rely on shared responsibility models where the cloud provider and the customer have security roles, necessitating different strategies for protecting data and managing security configurations.

? What should an organization's incident response plan for cloud security look like?

An effective cloud security incident response plan should include several critical components. To begin with, preparation involves assembling a skilled cloud security team, defining roles, and creating detailed incident response procedures for cloud environments. Identification follows, focusing on implementing advanced monitoring and detection tools to quickly spot anomalies and threats.

Next, containment strategies should limit the

impact by isolating affected resources and applying immediate controls. After this comes eradication, which requires identifying and removing the root cause, fixing vulnerabilities, and applying necessary patches. Recovery plans involve restoring systems and services to normal while ensuring data integrity, with regular backup and recovery testing. Additionally, communication protocols must address internal and external notifications, including stakeholders and regulatory bodies. The lessons learned should be analyzed post-incident to refine response strategies and improve security measures. Ultimately, the documentation of the incident and response actions are essential for compliance, legal purposes, and future reference.

? What are the best practices for securing data in the cloud?

Start with encryption, applying strong encryption protocols for data in transit and at rest, and manage encryption keys with strict security measures. Implement access controls through identity and access management (IAM), enforcing the principle of least privilege and regularly reviewing permissions to adapt to evolving roles. Also, conduct regular audits and vulnerability assessments to identify and address potential risks, leveraging automated tools for continuous monitoring. Establish a strong data backup strategy with automated, encrypted backups and regularly test recovery processes.

In addition to that, utilize multi-factor authentication (MFA) to add a layer of security beyond passwords. Keep systems up-to-date with patch management, ensuring all software and services are updated with the latest security patches. Develop and enforce comprehensive security policies covering data handling, storage, and sharing. Furthermore, protect network traffic with network security measures such as firewalls, VPNs, and intrusion detection systems (IDS). Invest in training and awareness programs to educate employees on best practices for cloud security and phishing prevention. Finally, maintain a robust incident response plan to quickly address and mitigate any security incidents, ensuring minimal impact and swift recovery.

? How can businesses assess the security posture of their cloud environments?

Businesses can start with security audits

and vulnerability assessments to identify weaknesses and misconfigurations. They can employ Cloud Security Posture Management (CSPM) tools for continuous monitoring and automated remediation of policy violations. They can also conduct penetration testing to simulate attacks and uncover potential vulnerabilities. It is necessary to ensure compliance with relevant regulations and standards through regular compliance checks. Enterprises must also evaluate risk by reviewing access controls, data protection measures, and incident response capabilities. They can implement security metrics and monitoring tools to track unauthorized access and anomalies. Engaging in third-party reviews for unbiased security assessments and expert recommendations is also crucial. Also, assess and enhance employee training on cloud security best practices to ensure internal teams are equipped to manage and mitigate risks effectively. This comprehensive approach provides a thorough evaluation of the cloud security posture and identifies areas for improvement.

? How are cloud security threats evolving, and what does the future hold?

As cloud technology advances and attackers become more sophisticated, one major trend we are seeing is the increase in targeted attacks, such as ransomware and advanced persistent threats (APTs), which exploit vulnerabilities in cloud environments to access critical data. Complex cloud architectures introduce new attack surfaces, making it harder to secure all components and manage configurations effectively. Moreover, the rise of serverless computing and containerization creates new security challenges, including securing ephemeral environments and managing container vulnerabilities.

The future of cloud security will likely see a greater emphasis on AI and machine learning for threat detection and response, enabling faster and more accurate identification of anomalies. Zero Trust models will become more prevalent, focusing on verifying every access request regardless of its origin. As cloud adoption grows, so will the need for integrated security solutions that provide comprehensive protection across multi-cloud and hybrid environments. Enhanced regulatory requirements and privacy concerns will drive innovations in security practices to address emerging threats and ensure compliance. ➡



DRIVING OPERATIONS AND PERFORMANCE EXCELLENCE

YOUR PARTNER FOR



Cloud & Digital
Transformation



Enterprise
Applications



Analytics &
Automation AI &
ML as a Service



Cyber
Security
Solutions



Management Consulting,
Advisory and Quality Assurance

An unit of



"Delivery centres in US, Middle East and India"

ELIMINATING AND AUTOMATING PERMISSION SPRAWL IN CLOUD ENVIRONMENTS

A new approach can reduce the number of access events to be managed in the cloud, by incorporating data awareness into access management processes and laying the foundation for a new security paradigm that supports contextual risk assessment and enforcement of least privilege, explains Maher Jadallah, Senior Director Middle East & North Africa, from Tenable.

As the definition of what constitutes a system, an application and even a user becomes increasingly blurred, providing secure access to cloud services for human and machine identities requires a shift that starts with the breakdown of traditional data and identity silos. Under the shared responsibility model for the public cloud, protecting identities and data is the responsibility of the enterprise rather than the cloud service provider. In any kind of cloud deployment model, even in Software as a Service, where the application layer security is managed by the cloud provider, customers are still required to protect their own data, identities and application

MAHER JADALLAH

Senior Director Middle East
North Africa,
Tenable





configurations.

The growing scale and complexity of public cloud deployments introduces security challenges for organizations that try to do their part in the shared responsibility model. Despite the abundance of identity-centric products, organizations still fail to provide protection for their critical assets.

Challenges of managing identity at cloud scale

Identities are a key component of any access security strategy. By assigning an identity to an entity, organizations can define access rights and permissions about what that entity can see and do.

With identity and access management (IAM) systems, organizations can centrally manage authentication and authorization across multiple systems and applications. Identity governance and administration (IGA) solutions provide additional capabilities across heterogeneous systems, for managing and governing the lifecycle of identities.

Privileged account management (PAM) addresses the specific need to manage and protect privileged accounts and credentials from being abused.

These identity-centric solutions could previously be utilized in the pre-cloud era as the slow pace of change enabled

administrators to keep things under control. But when organizations started adapting their IAM systems to operate in the cloud, they soon realized they were not sufficient for dealing with the huge volume of access rights that must be administered. The security industry has responded to the challenge by developing new solutions designed to operate in dynamic infrastructures at cloud scale.

The past few years have seen the emergence of various cloud extensions to IGA offerings. But they are not flexible enough to address the requirements of dynamic cloud environments consisting of multiple applications, each with their own authorization models.

In addition, alternatives have been developed to the traditional way of setting permissions based on roles, an approach that is too rigid and granular for cloud environments where roles are prone to frequent changes.

More advanced solutions utilize attribute-based or policy-based access control (ABAC or PBAC) that allow for managing permissions based on the user's actual behaviour, considering factors such as user location, time of access and device. Applying this approach across the enterprise to cover user-to-machine and machine-to-machine interactions in real-time, at cloud scale, is a challenge.

Disconnect between identities and data

Organizations are struggling to monitor interactions or access events, which can be defined as any request by a human or a machine to access a file or a resource for a certain purpose. A postmodern IT environment is emerging, with new types of identities and entities that interact with each other, and are often autonomous of human control.

Due to shorter build times and faster release cycles achieved through the use of DevOps tools, reorganizing permissions across identities and entities every time new code is deployed is a challenge.

But what if this burden could be eased through improved allocation of efforts and resources?

Even in complex cloud environments, most access events pose no risk at all as they involve neither sensitive data nor critical resources that might be compromised. What if organizations could identify risk-free access events to which organizations could automatically create and assign granular, unrestrictive policies and permissions? This will allow organizations to focus attention on those events where sensitive assets are involved or where organizations do not have enough immediate information at hand to decide.



This approach can reduce the number of access events to be managed. Incorporating data awareness into access management processes could lay the foundation for a new security paradigm that supports ongoing contextual risk assessment and effective enforcement of least privilege policies. As much as this might make sense, a solution based on an understanding of identities, integrated with data and resources is not practical with legacy products. In reality, identities and data are two different worlds that do not speak the same language.

Emergence of a new security model

As organizations are required to constantly adapt their policies and controls, IT and human resources and budgets are pushed to their limits.

Many organizations are approaching a tipping point where the scale and flexibility of cloud environments may be too much to deal with, resulting in exposure to risk. Even a single access-related incident due to an over-privileged account or a misconfigured cloud storage bucket may have consequences. The key to addressing the challenge of managing identities and permissions in the cloud at the user, application and resource level is to introduce automation, thereby reducing the level of required human resources.

By leveraging data-awareness, organizations can establish a decision-making framework that distinguishes between legitimate and

excessive permissions based on contextual understanding of the risk they pose to critical data or resources. This helps to enforce least privilege policies. By monitoring all access events, organizations can create a baseline of legitimate permissions and detect anomalies and threat activities at this scale.

Characteristics of the new model

Least privilege: Identities and entitlements are no longer static; therefore, policies should ensure users, applications, machines and services can access only data and resources that are necessary for their purposes.

A least privilege model for the cloud relies on the ability to continuously adjust access controls. The incorporation of data-awareness into an access management framework can improve the least privilege posture.

Automation: Automation is the prescription for scale issues. Given the number of entities, resources and permissions, the process of creating and enforcing least privilege policies, should be done rapidly, at scale and with minimal involvement of Dev or Ops teams. This way, organizations can achieve least privilege while allocating human resources to identify and resolve complicated permissions and investigate unknown access events.

Contextual policies: Not all access permissions are equal. Some are risky, others are not, while some others involve an unknown level of risk. Given the

number of access policies in modern cloud environments, organizations must be able to differentiate between how to manage them. The level of risk can be defined according to the sensitivity of the data, the resource where it resides, attributes of the entity that holds the permissions, its past behaviour, among others.

Secure access: Cloud data and resources are accessed by entities including human users, employees and customers, applications, computer-generated identities, microservices, IoT devices and more. Similar principles and logic should be applied to all entity types to ensure security across the cloud environment, without impacting application continuity or speed to market. Too often, user permissions are managed by IAM teams that struggle with modern cloud environments and focus on features that translate well from the on-premises realm.

Minimal disruption: To identify and mitigate access-related risks with minimum disruption to normal business operations, next-generation security systems should be able to enforce dynamic policies based on analysis of user behaviour, application requirements, and application and resource dependencies.

In summary, organizations should focus on leveraging automation and contextual data information at cloud scale to eliminate requests for changing privileges that are without risk, while identifying requests that require human intervention. 🔗

BREAKING NEW GROUND

Picus Security stands out in the crowded cybersecurity market by offering a unique and comprehensive approach to threat exposure management. Tarek Kuzbari speaks about what sets Picus apart from other cybersecurity vendors is its ability to correlate and aggregate data from various security silos, enabling a clear, prioritized view of risks based on business context.

? Can you provide an overview of Picus and its core cybersecurity solutions?

Picus Security, the leading security validation company, gives organizations a clear picture of their cyber risk based on business context. Picus transforms security practices by correlating, prioritizing, and validating exposures across siloed findings so teams can focus on critical gaps and high-impact fixes. With Picus, security teams can quickly take action with one-click mitigations to stop more threats with less effort.

Picus Security provides a threat exposure management solution, powered by our Exposure Data Fabric and Numi Ai™. The platform offers several capabilities including: breach and attack simulation, automated pentesting, cloud security validation, detection rule validation and attack surface management.

The pioneer of Breach and Attack Simulation, Picus delivers award-winning threat-centric technology that allows teams to pinpoint fixes worth pursuing, offering a 95% recommendation in the Gartner Peer Insights Review for the Breach and Attack Simulation category.

? What differentiates Picus from other cybersecurity vendors in the market?

The Picus Security Validation Platform is the only open-platform that allows security teams to correlate and aggregate data from various silos. We offer the ability to bring together vulnerability, attack surface and threat data so you can easily validate risk and take action with a short list of high-impact actions based on your business context. Picus offers top of the line vendor-specific mitigations to accelerate fixes in specific detection and prevention tools. With the Picus Threat Library and industry leading accuracy we virtually eliminate false-positives and save hours of manual research time.

? What kind of threats does Picus primarily focus on, and how effective are your solutions in mitigating them?

Picus Security focuses on mitigating a variety of cyber threats through advanced simulation and validation techniques. Our primary threat modules include:

TAREK KUZBARI

Regional Director Middle East and Africa,
Picus

1. Network Infiltration: Detects and prevents unauthorized access to your network.

2. Attack Scenarios: Simulates real-world attack scenarios to identify vulnerabilities.

3. Email Infiltration: Analyzes and blocks email-based attacks.

4. URL Infiltration: Identifies and prevents access to malicious websites.

These modules are updated weekly with the latest discovered threats, ensuring that our solutions are always current.

Picus solutions are highly effective in both the **prevention** and **detection** layers. We provide action-based mitigation recommendations for each threat. These recommendations help you quickly and effectively close security gaps, minimizing your cyber risk.

For example, when a new network infiltration method is discovered, Picus simulates the attack, assesses how well your current security measures can handle it, and offers detailed recommendations on how to prevent it. This proactive approach ensures that your security measures remain effective against constantly evolving threats.

Picus solutions help organizations improve their security posture proactively, making them more resilient against cyber threats.

? Can you describe the role of AI and machine learning in your cybersecurity solutions?

- **Picus Numi AI™**: provides security teams with easy access to up-to-date information about their organization's security posture and recommends ways to enhance resilience against the latest threats.

- **AI-driven Threat Profiling:** curates cyber threat intelligence from hundreds of data sources to deliver up-to-date information about threats and guide security validation activities based on industry, geography, and other factors.

- **AI-based MITRE ATT&CK Mapping:** enables users to visualize the detection coverage provided by SIEM tools by automatically mapping detection rules to the MITRE ATT&CK Framework and supplying AI-based technique suggestions for unmapped rules.

? What are the current trends in cybersecurity that organizations should be aware of?

Today Security practitioners continue to be challenged with the ability to resource their teams effectively to cover the widening attack surface posed by digital transformation, the

journey to the cloud and the rapid evolution AI poses. These industry evolutions are sparking key trends including the use of AI as a catalyst to augment security teams, and the use of Exposure Validation to complete a more proactive approach to security posture using the framework of Continuous Threat Exposure Management (CTEM). The best defense is a good offense. As security teams work smarter they will soon have a better understanding of their validated risk level, and the ability to think like an attacker, which allows them to use offenses to prepare their defenses.

? How does Picus stay ahead of emerging threats and adapt its solutions accordingly?

Picus Security stays ahead of emerging threats and continuously adapts through a combination of advanced technology, continuous updates, and expert insights from Picus Labs. Here's how we achieve this:

1. Picus Threat Library:

- Updated daily by our team of offensive security experts, our threat Library is one of the most comprehensive and up-to-date in the industry. It includes over 4,000 threats and 19,000 actions.

- New threats are added to the library within 24 hours of their disclosure, ensuring our simulations reflect the latest attack techniques. These threats are mapped to frameworks such as MITRE ATT&CK, OWASP, CVE, and CWE, providing detailed references and context

2. Picus Labs:

- Picus Labs, our dedicated research and development team, plays a crucial role in identifying and analyzing new threats. They continuously monitor the cyber threat landscape to discover emerging threats and integrate this knowledge into our platform.

- The lab's efforts ensure that our attack simulations are always relevant and reflective of real-world scenarios, helping organizations stay prepared against the latest threats.

3. Continuous Security Validation:

- Our platform continuously validates the effectiveness of your security controls by simulating real-world cyber threats. This approach helps identify prevention and detection gaps, providing actionable mitigation recommendations to address them swiftly and effectively

- By automating these validation processes, Picus reduces the time and effort required for manual assessments, allowing your security team to focus on remediation rather than

discovery

4. Modular and Flexible Solutions:

- Picus offers a modular design with individually licensable products and attack modules, enabling you to customize the solution to your specific needs. This flexibility ensures that you can target the most relevant threats to your environment and continuously improve your security posture.

5. Integration with Security Tools:

- Picus integrates with a wide range of network and endpoint security tools, streamlining workflows by automating the application of mitigation content. This integration ensures that your security controls are always tuned to block the latest threats

By leveraging these capabilities, Picus Security ensures that organizations are proactive and resilient against the ever-evolving threat landscape. Our continuous updates, expert insights, advanced simulation technologies and attack path validation provide a clear view of validated risk and allow teams to pinpoint what is needed to maintain their security posture.

? What are the biggest challenges organizations face today in cybersecurity, and how does Picus address them?

Organizations today have several challenges that are everlasting due to the evolving threat landscape, alert fatigue and general resource deficiencies. However the real challenge lands with their inability to understand their current cyber risk and how to address current gaps in cybersecurity.

Every organization has a chance of a breach and are working to reduce that chance. To do that they must answer 2 questions: What is our risk level? And, what do we focus on to reduce it? Picus helps security teams address these questions with a way to validate if the thousands of vulnerabilities and exposures they look at on a weekly basis are truly a source of risk. While you may have 100K vulnerabilities in your backlog, it could be that only a fraction of these are worth spending your time on. Picus correlates siloed vulnerability, attack surface and validation data with business context to pinpoint the exposures that truly pose a risk, so security teams can spend time on threats worth pursuing and deploy them fast. When you know exactly what to fix, you can reduce your risk of breach.

? How customizable are your solutions to fit the

specific needs of different industries or organizations?

Picus Security's solutions are highly customizable to meet the specific needs of different industries and organizations, they include:

1. Modular Design: Our platform offers individually licensable products and attack modules, allowing you to tailor the solution to your specific needs. They can be used together, or alone to right size the requirement of the business.

2. Comprehensive Threat Simulation: We simulate a wide range of threats, including industry-specific attacks, ensuring relevance to a broad range of industries.

3. Vendor-Specific Mitigation: We provide tailored prevention signatures and detection rules based on your existing security toolset.

4. Integration with Existing Tools: Our platform integrates seamlessly with a wide range of security tools, enhancing your current security infrastructure without major changes.

5. User-Friendly Interface: An intuitive interface and customizable dashboards make it easy to schedule simulations and view results tailored to your needs.

Picus ensures your organization receives a tailored security solution, enhancing your defense against industry-specific threats.

? What is Picus's roadmap for future product development and innovation?

Picus Security is committed to staying ahead of the ever-evolving cyber threat landscape by continuously innovating and enhancing our platform. Our roadmap for future product development focuses on several key areas:

1. Enhanced AI and Machine Learning Capabilities:

We are investing heavily in AI and machine learning to further enhance our platform's capabilities. This includes improving our Numi AI™ virtual security assistant to provide even more accurate and actionable insights, helping organizations make faster and more informed decisions. ➡

2. Deeper Integration with Security Tools:

We continue to expand integrations with a wider range of security tools and platforms, similar to our one-click auto-deploy integration with CrowdStrike. This will provide our customers with greater flexibility and interoperability, allowing them to seamlessly incorporate Picus into their existing security ecosystems.

3. Expansion of Threat Library:

We plan to continuously expand our threat library, ensuring that it includes the latest and most relevant threats. Our goal is to simulate over 30,000 threats and tactics, techniques, and procedures (TTPs) by the end of next year, maintaining our position as a leader in threat simulation and validation.

4. Cloud and Container Security:

We are focusing on enhancing our capabilities in cloud and container security. This includes developing new modules specifically designed to address the unique challenges of securing cloud-native environments and containerized applications.

5. Improved User Experience:

We are committed to making our platform even more user-friendly and intuitive. This includes redesigning our user interface to provide a more streamlined and efficient user experience, as well as enhancing our dashboards and reporting capabilities.

6. Advanced Analytics and Reporting:

We have introduced advanced analytics and reporting features, enabling organizations to gain deeper insights into their security posture and the effectiveness of their controls. This addition to our platform will continue to evolve and identify trends, measure improvements, and demonstrate value to stakeholders.

? How do you foresee the cybersecurity landscape evolving over the next 5-10 years?

Over the next 5-10 years, the cybersecurity landscape will undergo significant transformations due to AI developments and higher saturation of cloud adoption. Continuous Threat Exposure Management (CTEM) will also become a cornerstone of cybersecurity strategies, with Gartner predicting that 60% of organizations will adopt CTEM by 2025, up from less than 10% in 2021. This shift is expected to reduce security incidents by 30% due to improved detection and remediation capabilities.

AI and machine learning will play a crucial role in enhancing threat detection, predictive analytics, and automated responses, thereby reducing the burden on security teams and improving overall efficiency. With AI automation in the security operations team will advance and alleviate some of the burden on security teams so they can focus on key exposures that pose elevated risk.

Stringent data protection regulations will drive organizations to adopt robust security

measures, requiring continuous validation of security controls and comprehensive reporting capabilities. The focus will shift from solely preventing attacks to ensuring cyber resilience, maintaining operations, and recovering quickly from incidents. By embracing these trends and adopting advanced exposure management practices, organizations can stay ahead of emerging threats and maintain a robust security posture in the evolving cybersecurity landscape.

? Can you share highlights from the latest Blue Report?

The Blue Report 2024: State of Exposure Management* revealed 40% of tested environments allowed attack paths that lead to domain admin access. Achieving domain admin access is like giving attackers a master key to an IT organization, which is highly concerning. The report, based on a worldwide comprehensive analysis of more than 136 million cyber attacks simulated by the Picus Security Validation Platform.

Well over a third (40%) of environments have weaknesses that allow attackers with initial access to a network to achieve domain admin privileges. Once they have these privileges they can manage user accounts or modify security settings. A compromised domain admin account can lead to full control of the network, allowing attackers to conduct data exfiltration, deploy malware, or disrupt business operations.

The report also reveals that on average, organizations prevent 7 out of 10 of attacks, but are still at risk of major cyber incidents because of gaps in threat exposure management that can permit attackers using automation to move laterally through enterprise networks. Of all attacks simulated, only 56% were logged by organizations' detection tools, and only 12% triggered an alert.

"Like a cascade of falling dominoes that starts with a single push, small gaps in cybersecurity can lead to big breaches," said Dr. Suleyman Ozarslan, Picus co-founder and VP of Picus Labs. "It's clear that organizations are still experiencing challenges when it comes to threat exposure management and balancing priorities. Small gaps that lead to attackers obtaining domain admin access are not isolated incidents, they are widespread.

Last year, the attack on MGM used domain admin privileges and super admin accounts. It stopped slot machines, shut down virtually all systems, and blocked a multi-billion dollar company from doing business for days." ➡

THE SHIFTING SANDS OF CYBERSECURITY

Ricardo Ferreira, EMEA Field CISO at Fortinet, throws light on new and emerging cybersecurity threats and attacker tactics.

As cyberthreats continue to evolve nearly four decades after the first computer virus for PCs emerged in 1986, the cybersecurity landscape faces increasingly sophisticated challenges. While many are familiar with common threats like phishing and ransomware, newer, more targeted attacks are emerging, threatening the very foundations of our digital infrastructure.

Supply Chain Cyber Risks

Recent incidents have underscored the devastating potential of supply chain attacks. One alarming example is the XZ Utils backdoor (CVE-2024-3094), a critical vulnerability found in a widely used open-source compression tool. This attack, led by the “Jia

A portrait of Ricardo Ferreira, a man with dark, wavy hair and a beard, smiling. He is wearing a white button-down shirt. The background is plain white.

RICARDO FERREIRA,
EMEA Field CISO,
Fortinet



Tan” account, was a multi-year operation that began in 2021 and culminated in deploying a backdoor in 2024. Over time, the attackers embedded their exploit into the software, demonstrating how deeply supply chain attacks can infiltrate and exploit foundational software used across numerous organizations. This incident serves as a critical reminder for organizations to scrutinize the security of their software supply chain. Open-source components can be weak links often maintained by small and underfunded teams. Organizations must monitor updates and patches to avoid introducing new vulnerabilities.

Open-Source Software Issues

The XZ Utils incident highlights broader concerns within the open-source community. Malicious actors can insert backdoors into open-source projects with alarming ease. The Jia Tan account is just one example of how suspicious accounts can fly under the radar, quietly injecting malicious code into widely used software packages.

A recent analysis revealed that even PIP, the Python package management system, has a suspicious account with commit access. This raises serious concerns about the security of numerous critical Python packages. These accounts often make seemingly innocent contributions but could lay the groundwork for future exploits. This situation underscores the need for greater vigilance and verification within the open-source community. Organizations relying on open-source software must implement strict vetting processes and use tools to monitor and alert them to suspicious activity within their codebases.

The Promise and Perils of GenAI

GenAI offers transformative potential, as demonstrated by Klarna’s AI Assistant, which now handles the workload equivalent to 700 customer service agents. For Klarna, this translates into an estimated \$40 million in annual savings, showcasing AI’s ability to enhance productivity and reduce operational costs.

However, the integration of GenAI comes with risks. Executives need to ensure that cybersecurity is a foundational consideration when adopting AI solutions. GenAI systems can be vulnerable to various threats, such as data poisoning, where attackers feed misleading data into AI systems, resulting in incorrect outputs. Additionally, these systems can face denial-of-service attacks, increasing costs and degrading performance, or privacy breaches where sensitive data is exposed.

Three key considerations when integrating GenAI are availability, system integrity, and privacy. Ensuring these aspects are robustly managed will help mitigate the risks associated with deploying AI systems at scale.

Best Strategic Defense Tactics against Cyberattacks

Organizations must adopt a multi-layered defense strategy to navigate this complex threat landscape. Here are some critical components:

1. Proactive security testing: red and blue team exercises

Red and blue team exercises simulate real-world cyberattacks, helping organizations uncover vulnerabilities before they can be exploited. For AI systems, these exercises should focus on assessing the robustness of

models against harms such as hallucination, bias, and prohibited content like harassment. Organizations can stay ahead of potential threats by continuously evaluating and improving the security and ethical performance of AI systems.

2. AI-specific security measures, start leveraging ATLAS

Addressing AI-specific threats is crucial as AI becomes more integrated into business processes. Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS) is a knowledge base complementary to MITRE ATT&CK that documents real-world adversarial tactics against AI systems. Organizations should use ATLAS to stay informed about these evolving threats and improve their defenses against attacks targeting AI technologies.

3. Zero-trust architecture, the journey to better access control

Adopting a zero-trust architecture is crucial in today’s environment, especially for systems integrating AI. This approach operates on the principle that no entity—whether inside or outside the network—should be trusted by default. Continuous verification of user identities and strict access controls are foundational elements.

However, for AI systems, data boundaries are equally important. AI models often process vast amounts of sensitive data, and ensuring that this data is adequately segmented and protected is critical. Establishing clear data boundaries prevents unauthorized access to sensitive information, reducing the risk of data leakage or manipulation. This is particularly vital in AI systems where data integrity directly impacts the outputs and decisions made by the AI.

By implementing a zero-trust architecture with strong data boundary controls, organizations can ensure that their AI systems operate securely, protecting both the data they process and the insights they generate.

The evolving threat landscape demands that organizations remain vigilant and proactive in their cybersecurity efforts. Organizations can better protect their digital assets by understanding the risks associated with supply chain vulnerabilities, open-source software, and the integration of GenAI, as well as by implementing strategic defense tactics. Cybersecurity is no longer just an IT issue. It’s a critical component of overall business strategy that requires attention at every level of the organization. 🔒

IDENTITY AT THE CORE

Christopher Hills, Chief Security Strategist, BeyondTrust, why stronger identity and access management needs both provisioning and deprovisioning.

Across the Middle East, CIOs and CISOs huddle together to determine ways of making their organizations more secure so that digitalization can align with the vision of business leaders. No enterprise can afford to shut itself off from the digital economy. Whether it operates locally, regionally or globally, a business must build trust. And to do that, it must master the art of identity management. Therefore, it must understand the importance of provisioning and deprovisioning.

Provisioning is the name we give to the granting of privileges. This is a more granular process than onboarding, in which a new user account is created. Each user may have privileges granted at any time.

CHRISTOPHER HILLS,
Chief Security Strategist,
BeyondTrust



And we should remember that not all users are humans — employees, contractors, customers, and so on. Privileges may be assigned to service accounts, machinery, and other resources. The purpose of provisioning is to maintain access while accounting for security and compliance standards.

To meet modern security standards, however, deprovisioning is just as important. Again, this does not just occur during offboarding. Privileges can be revoked all the time. Not because of a loss of trust in the person or asset that held them, but because it is best practice. Effective provisioning and deprovisioning is the foundation of a robust identity-centric security solution.

Covering the bases

Both are important. Overprovisioning can lead to a junior employee or overlooked service having unnecessary privileges, and under-deprovisioning can lead to a range of invisible issues such as unmonitored or orphaned accounts, or stale privileges. Special care must also be taken when adding or removing accounts to user groups — which carry with them a predetermined set of privileges — because these actions amount to provisioning and deprovisioning.

Any active account is a potential entry point, so it should come as no surprise that security best practice lies in minimizing the number of accounts and the access privileges they hold. If an account is no longer needed — an employee has resigned, a project has come to an end, or a range of other scenarios — then it should be disabled, deleted, or its rights downsized. Threat actors rely on organizations not following this simple practice. And regulators take a dim view of the same. These two reasons alone should spur regional organizations to implement best practices for provisioning and deprovisioning.

Part of IAM 101 is the principle of least privilege (PoLP), which dictates that any human or non-human account be granted only enough access to perform the function of its owner. In the provisioning phase, the role of the owner should be considered. Role-based access control will allow precision in the assignment of privileges. It will deliver the ability to monitor and audit all activity. And it will simplify the tracking and updating of permissions as roles change.

Tools and tricks

Robust IAM will also include just-in-time (JIT) provisioning, which goes hand in hand



with PoLP. When deprovisioning occurs, the timely revocation of access also occurs. Regularly reviewing and adjusting access rights is best practice because it prevents unnecessary permissions being exploited by malicious parties inside or outside the organization. All unused accounts should be placed in a disabled state and removed from all relevant security groups until such time as they can be reviewed and, if appropriate, deleted.

Identity and access management cannot be effective without the right tools to simplify provisioning and deprovisioning. This is because looking after the end-to-end lifecycle of identities, privileges, and entitlements is a complex task that has grown even more complex since the region's mass migration to hybrid and multi-cloud environments. Identity management tools can streamline the creation, maintenance, and deletion of human and non-human accounts. Governance management tools enforce policies that limit access based on the assigned privileges. Lifecycle management tools are useful for ensuring (from onboarding to offboarding) that privileges always fit the role of an account owner. Privileged access management (PAM) enforces PoLP and provides a useful integration hub for other tools so that IT and security teams have single-pane control over everything that may impact identity security.

In a modern setting, provisioning and deprovisioning tools must offer automation and user behavior analytics, which means they must incorporate some flavor of AI or machine learning. To be consistent with the implementation of PoLP and other governance policies, variants of AI are necessary to minimize human error. Granting and revoking

access rights in a company of even moderate size is a constant process that responds to changes in personnel and circumstances. While some of these situations may be subject to planning, others, such as real-time behavioral anomalies, are not. Threats can arise at a moment's notice and only AI offers a practical option for timely response.

Be strong

Having established provisioning and deprovisioning as the keys to strong IAM, enterprises will find they can implement more effective lifecycle management of identities, privileges, and entitlements. As with any new measure, ongoing reviews will uncover any additional requirements, and adjustments can be made to cover new regulations, new assets, or new business models. As the identity landscape fluctuates, so should provisioning and deprovisioning strategies.

Define roles clearly. If an account owner does not need access to a resource, do not grant it (PoLP); and if they do, wherever possible, grant access only for as long as it is required (JIT). Disable and delete accounts where appropriate and monitor access across the entire ecosystem as often as is practical — quarterly or annually. Following the guidance laid out here will strengthen your identity security posture. The modern threat actor is always on the lookout for gaps in your defenses. Unfortunately, these often take the shape of overprovisioned identities or abandoned accounts that have not been adequately addressed. The good news is that by applying the steps above, you can shore up defenses and protect the enterprise from the worst of the threats beyond its walls. 🏠



THE NEW OPTIPLEX FAMILY

INTELLIGENCE MEETS SIMPLICITY

Dell's new desktops are redesigned and simplified to make finding your perfect match easier than ever. The new OptiPlex family features Windows 11 Pro, AI-personalization from the latest Optimizer, one BIOS for all-in-ones and one BIOS for towers. Find the OptiPlex that fits your workstyle now.



Dell Technologies recommends
Windows 11 Pro for business



CLOUDFLARE REPORT: ORGANIZATIONS STRUGGLE WITH OUTDATED SECURITY AMID RISING ONLINE THREATS

A portrait of Matthew Prince, Co-founder and CEO of Cloudflare. He is a middle-aged man with short, wavy brown hair and a friendly smile, showing his teeth. He is wearing a dark blue or black blazer over a black t-shirt. The background is plain white.

MATTHEW PRINCE,
Co-founder and CEO,
Cloudflare



Cloudflare's State of Application Security 2024 Report reveals that security teams are struggling to manage risks from modern applications. The report highlights the increasing volume of threats from software supply chain issues, DDoS attacks, and malicious bots, often exceeding the resources of dedicated application security teams. Today's digital world runs on web applications and APIs. They allow ecommerce sites to accept payments, healthcare systems to securely share patient data, and power activities we do on our phones. However, the more we rely on these applications, the more the attack surface expands. This is further magnified by the demand for developers to quickly deliver new features—e.g., capabilities driven by generative AI. But if unprotected, exploited applications can lead to the disruption of businesses, financial losses, and the collapse of critical infrastructure.

"Web Applications are rarely built with security in mind. Yet, we use them daily for all sorts of critical functions, making them a rich target for hackers," said Matthew Prince, co-founder and CEO at Cloudflare.

"Cloudflare's network blocks an average of 209 billion cyber threats for our customers every single day. The layer of security around today's applications has become one of the most essential pieces to making sure the Internet stays secure."

Key findings from Cloudflare's State of Application Security 2024 Report include: DDoS attacks continue to increase in number and volume: DDoS remains the most leveraged threat vector to target web applications and APIs, comprising 37.1 % of all application traffic mitigated by Cloudflare. Top targeted industries were Gaming and Gambling, IT and Internet, Cryptocurrency, Computer Software and Marketing and Advertising. First to patch vs. first to exploit—the race between defenders and attackers accelerates: Cloudflare observed faster exploitations than ever of new zero-day vulnerabilities, with one occurring just 22 minutes after its proof-of-concept (PoC) was published. Bad bots—if left unchecked—can cause massive disruption: One-third (31.2%) of all traffic stems from bots, the majority (93%) of which are unverified and potentially

malicious. Top targeted industries were Manufacturing and Consumer Goods, Cryptocurrency, Security and Investigations, and US Federal Government.

Organizations are using outdated approaches to secure APIs: Traditional web application firewall (WAF) rules that use a negative security model—the assumption that most web traffic is benign—are most commonly leveraged to protect against API traffic. Far fewer organizations use the more widely accepted API security best practice of a positive security model—strict definitions on traffic that is allowed, rejecting the rest. Third-party software dependencies pose growing risk: Organizations use an average of 47.1 pieces of code from third-party providers and make an average of 49.6 outbound connections to third-party resources to help enhance website efficiency and performance—e.g., leveraging Google Analytics or Ads. But as web development has largely shifted to allow these types of third-party code and activity to load in a user's browser, organizations are increasingly exposed to supply chain risk and liability and compliance concerns. [➡](#)

GITEX

G L O B A L

14 - 18 OCTOBER

DUBAI WORLD TRADE CENTRE

MON
11 AM - 5 PM

TUE - FRI
10 AM - 5 PM

THE LARGEST TECH & STARTUP
EVENT IN THE WORLD

Global Collaboration to Forge a Future AI ECONOMY

6,700⁺

Exhibitors

187k

Visitors

1,800⁺

Speakers

Where the visionaries and policy makers meet.

#GITEXGLOBAL
gitex.com



Scan the QR code to

SECURE YOUR PASS



ORGANISED BY



مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

HUMAN RISK MANAGEMENT: THE NEXT STEP IN MATURE SECURITY AWARENESS PROGRAMS

In today's digital landscape, organizations face a myriad of security threats that evolve constantly. Among these threats, human risk remains among the most significant and challenging to mitigate. Human Risk Management (HRM) is the next step for mature Security Awareness Programs. HRM is an approach that focuses on understanding, managing, and reducing the risks posed by human behavior within an organization. Unlike traditional compliance training programs that rely solely on annual computer-based training, HRM is a comprehensive strategy to secure the workforce by fostering a strong security culture and changing employee behavior.

What is Human Risk Management?

Human Risk Management is a holistic approach to cybersecurity that goes beyond mere awareness. It encompasses various methods and practices designed to understand the human element in security, identify vulnerabilities, and implement strategies to mitigate risks.

HRM involves continuous education, regular engagement, and behavior modification techniques to ensure that employees not only understand security policies but also embody them in their daily activities.

The Importance of Human Risk Management

Despite advancements in technology and automated security measures, human error remains a predominant cause of security

A portrait of Lance Spitzner, a man with short brown hair and a goatee, smiling. He is wearing a grey crew-neck shirt. The background is white.

LANCE SPITZNER,
Security Awareness Director,
SANS Institute



breaches. Employees may fall victim to phishing attacks, use weak passwords, or inadvertently disclose sensitive information. HRM aims to minimize these errors by instilling a culture of vigilance and accountability.

Moreover, cyber threats are constantly evolving. What was a secure practice yesterday may not be sufficient today. HRM ensures that employees are regularly updated on the latest threats and best practices, making the workforce adaptable to new security challenges.

A strong security culture is one where security is ingrained in the organizational ethos. HRM helps in building such a culture by promoting shared values, beliefs, and practices regarding security. This cultural shift is crucial for long-term resilience against cyber threats.

While compliance with regulations and standards is essential, HRM focuses on building security into the fabric of the organization. This proactive approach not only meets compliance requirements but also enhances overall security posture.

HRM vs. Traditional Compliance Driven Programs

Traditional compliance programs often consist of periodic training sessions that employees must complete to comply with organizational policies. While these programs are necessary, they are not sufficient for mitigating human risk effectively.

And this is how HRM differs – HRM is an ongoing process that involves continuous learning and engagement. Instead of one-off training sessions, HRM includes regular workshops, phishing simulations, interactive seminars, and real-time feedback. This constant engagement helps in reinforcing good security practices and keeping security top of mind for employees.

The core of HRM is behavioral change. It uses psychological principles to understand why employees might engage in risky behaviors and employs strategies to modify those behaviors. Techniques such as positive reinforcement, gamification, and peer influence are used to encourage secure behavior.

HRM recognizes that one size does not fit all. Different employees have different roles, responsibilities, and levels of access to sensitive information. HRM tailors role-based security training and communication to address the specific needs and risks associated with each role, making the training more relevant and effective.

Ultimately, effective HRM also involves measuring the impact of training and engagement activities. Metrics such as phishing test results, incident reports, and employee feedback are analyzed to assess the effectiveness of the HRM program and identify areas for improvement.

Driving a Strong Security Culture

A strong security culture is the ultimate goal

of Human Risk Management, characterized by several aspects. Senior leadership must champion the cause of security, setting the tone for the entire organization. Their involvement demonstrates the importance of security and encourages employees to take it seriously.

Encouraging open communication about security issues helps in creating a supportive environment where employees feel comfortable reporting suspicious activities without fear of retribution. Additionally, empowering employees with the knowledge and tools they need to protect themselves and the organization is key. This includes not only technical training but also fostering a sense of ownership and responsibility for security. Recognizing and rewarding employees who demonstrate good security practices can motivate others to follow suit. This positive reinforcement helps in embedding security into the organizational culture.

Human Risk Management is a critical component of an organization's overall cybersecurity strategy. By going beyond just annual training and focusing on continuous engagement, behavioral change, and building a strong security culture, HRM effectively reduces the risks posed by human behavior. For senior leadership, investing in HRM is investing in the long-term security and resilience of the organization. It is about creating an environment where every employee understands their role in protecting the organization and is committed to maintaining a secure workplace. 

A Strategic Imperative

TechOps

Streamline their IT infrastructure and improve operational efficiency, which can result in lower costs and increased productivity.



Competency Framework

Assess your current capabilities architecture and identify areas for improvement, helping you to make informed decisions about where to invest your technology resources



TechSust Align

Optimize and improve your technology systems, ensuring they are operating at peak efficiency and effectively supporting your business goals.



Biz Insights

Provide advanced analytics services, leveraging the latest technologies and techniques to help you turn your data into actionable insights.



DXT

Develop a digital strategy that aligns with your business objectives, enabling you to stay ahead of the curve in a rapidly changing digital landscape.



POWERED BY

BOTS

GLOBAL
CIO
FORUM



THE
WORLD
CIO 200
SUMMIT

2024 ROADSHOW

MAY - SEPTEMBER 2024

UNLEASH THE MIGHT



50

COUNTRIES

4000

C-LEVEL EXECS

300+

SESSIONS

200+

EXHIBITORS