ISSUE 85 | JUNE 2024

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST

THE TRUST FACTOR

SECURITY ADVISOR MIDDLE EAST EXAMINES THE INCREASING RELEVANCE OF THE ZERO TRUST APPROACH IN BUILDING A ROBUST DEFENSE AGAINST ADVANCED CYBERTHREATS.

tahawultech.com

cnme
computer news middle east
SUPPLEMENT

CONTROL ACROSS THE NETWORK

Nuclias is an end-to-end solution. Whether you have a small chain of coffee shops, a bustling hotel, or even a college campus to cover, Nuclias offers the enterprise-grade hardware, software, and reliability you need to provide a seamless connected experience – indoors and outdoors.

Network management solutions for small-to-medium-sized businesses (SMBs).

Has network control ever been easier?

Download the app now and get started.

Nuclias Cloud

connect

Nuclias Connect

Download on the App Store

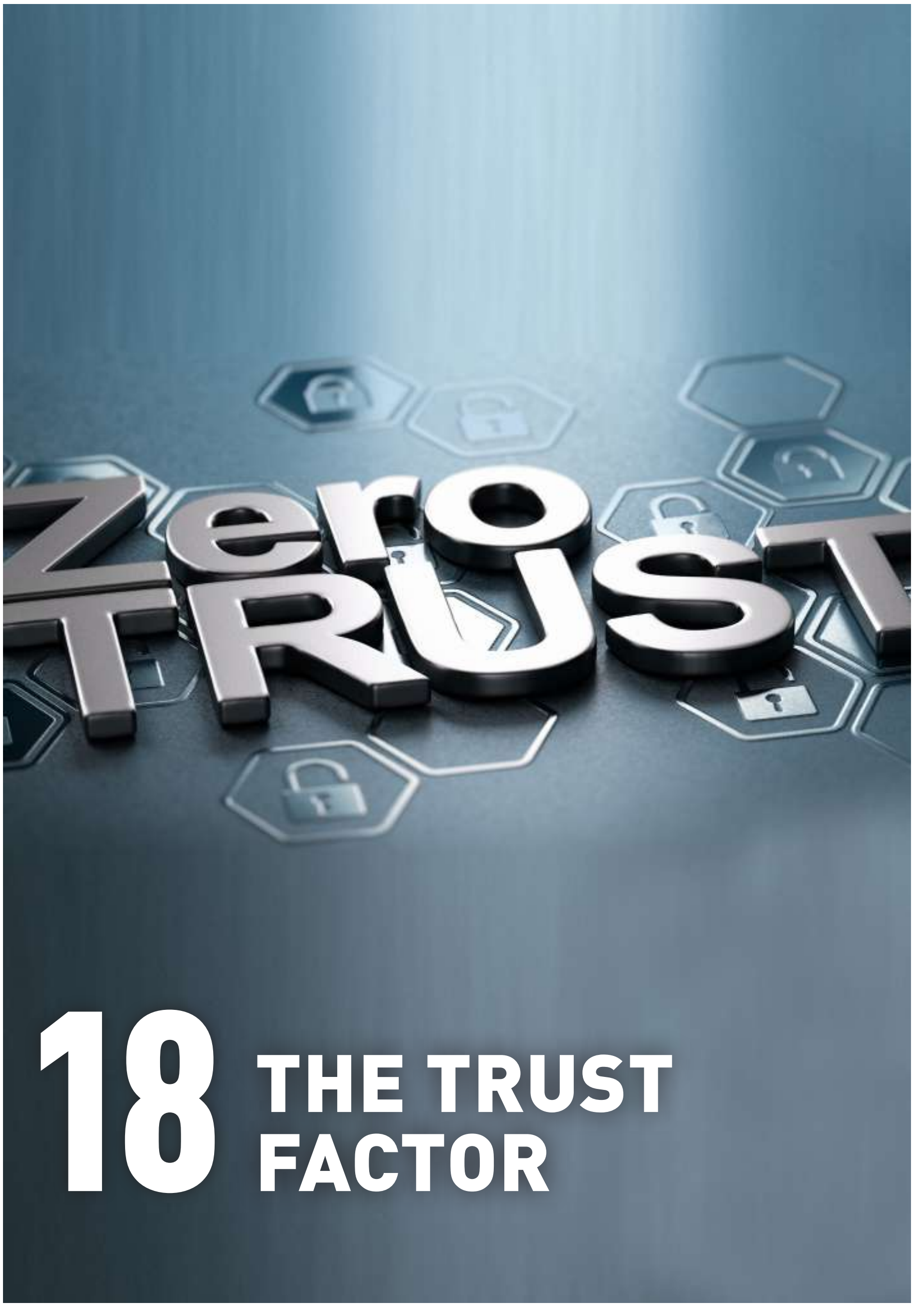
GET IT ON Google Play

nuclias

by D-Link®

CONTENTS

Security ADVISOR MIDDLE EAST



10

24

34

EDITOR'S NOTE

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

Anita Joseph
Editor

THE FUTURE OF CYBERSECURITY

As we stand on the precipice of a new digital age, the importance of cybersecurity cannot be overstated. With every passing day, the digital landscape evolves, presenting new opportunities and challenges. As artificial intelligence, the Internet of Things (IoT), and quantum computing become more integrated into our daily lives, the need for robust cybersecurity measures grows exponentially.

One of the most pressing issues is the sophistication of cyber threats. Cybercriminals are continually developing more advanced techniques to breach security systems, often outpacing traditional defensive measures. The rise of AI-powered cyberattacks, capable of learning and adapting, poses a significant threat to even the most secure networks. This necessitates a shift towards more dynamic and intelligent defense mechanisms, utilizing AI and machine learning to predict and counteract potential threats in real-time.

THE HUMAN ELEMENT IN CYBERSECURITY

The expansion of IoT devices presents another layer of complexity. With billions of connected devices, each potentially serving as a gateway for cyber threats, securing these networks is a monumental task. The future of cybersecurity will undoubtedly focus on creating standardized protocols and robust encryption methods to protect these devices from exploitation.

Quantum computing, while still in its infancy, represents both a threat and an opportunity. On one hand, quantum computers could potentially break current encryption methods, rendering traditional cybersecurity obsolete. On the other hand, they offer the promise of developing unbreakable encryption, ensuring data security in unprecedented ways. The race to achieve quantum supremacy will likely dictate the future landscape of cybersecurity.

Finally, the human element remains a critical factor. Cybersecurity is not just about technology but also about awareness and education. Building a culture of cybersecurity, where individuals are knowledgeable and vigilant, will be key to combating the ever-evolving threats.

In this rapidly changing environment, staying ahead of cyber threats requires continuous innovation and collaboration. The future of cybersecurity lies in our ability to anticipate, adapt, and educate, ensuring that our digital world remains secure for generations to come.

EVENTS

tahawultech.com
FUTURE SECURITY
AWARDS

tahawultech.com
CISO50
AWARDS & FORUM

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by CPI

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

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

EDITORIAL
Editor
Anita Joseph
anita.joseph@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

PRODUCTION AND DESIGN
Designer
Prajith Payyapilly
prajith.payyapilly@cpimediagroup.com

DIGITAL SERVICES
Web Developer
Adarsh Snehajan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

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.

ESET LAUNCHES AI ADVISOR TO ENHANCE THREAT DETECTION AND RESPONSE

ESET, a global leader in cybersecurity solutions, is proud to introduce ESET AI Advisor, an innovative generative AI-based cybersecurity assistant that transforms incident response and interactive risk analysis. First showcased at RSA Conference 2024, the new solution is now available as part of the ESET PROTECT MDR Ultimate subscription tier and ESET Threat Intelligence.

Unlike other vendor offerings and typical generative AI assistants that focus on soft features like administration or device management, ESET AI Advisor seamlessly integrates into the day-to-day operations of security analysts, conducting in-depth analysis. Building on over two decades of ESET's expertise in AI-driven endpoint protection, the offering provides detailed incident data and offers SOC team-level advisory. This is a gamechanger for companies with limited IT resources who want to utilize the advantages of advanced Extended Detection and Response (XDR) solutions and threat intelligence feeds.

"As cybersecurity threats become increasingly sophisticated, ESET remains committed to providing cutting-edge solutions that address these challenges. The ESET AI Advisor module represents a significant leap forward in our mission to close the cybersecurity skills gap and empower organizations to safeguard their digital assets effectively," said Juraj Malcho, Chief Technology Officer at ESET.

One of its primary benefits for this new solution is closing the cybersecurity skills gap. Security analysts of all skill levels can use ESET AI Advisor to conduct interactive risk identification, analysis, and response capabilities, which are provided in an easily understandable format. The user-friendly interface makes sophisticated threat data actionable even for less experienced IT and security professionals.

AMIVIZ PARTNERS WITH BITSIGHT TO ENHANCE CYBER RISK MANAGEMENT IN THE MIDDLE EAST

AmiViz, the first B2B enterprise marketplace for the cybersecurity industry in the Middle East, is proud to announce its partnership with Bitsight, the leader in cyber risk management. This collaboration marks a significant step forward in bolstering cybersecurity capabilities across the region and facilitating Bitsight's expansion efforts in the Middle East.

The partnership between AmiViz and Bitsight will enhance the cybersecurity landscape in the Middle East by introducing state-of-the-art solutions designed to tackle the evolving cyber threats confronting regional organizations. With both companies committed to improving cybersecurity awareness and resilience, they are set to pave the way for a safer and more secure digital environment in the region.

Commenting on the partnership with Bitsight, Ilyas Mohammed, COO at AmiViz said "Our decision to onboard Bitsight demonstrates our commitment towards the evolution of the cybersecurity landscape in the Middle East. As organizations grapple with increasingly sophisticated cyber threats, the partnership between these two industry leaders promises to deliver enhanced value by equipping organizations with the tools and insights needed to effectively manage cyber risks and safeguard their digital assets in an ever-evolving threat landscape."

Bitsight's solutions can proactively assess and manage their cyber risk exposure and provide organizations with actionable intelligence to optimize their security investments, streamline vendor risk management processes, and enhance cyber resilience. With a focus on continuous monitoring and data-driven insights, Bitsight empowers organizations to make informed decisions and stay ahead of emerging cyber threats.

ACRONIS EXPANDS ITS SECURITY OFFERING BEYOND ENDPOINT PROTECTION WITH NEW EXTENDED DETECTION AND RESPONSE (XDR) SOLUTION

Acronis, a global leader in cybersecurity and data protection, has introduced Acronis XDR the newest addition to the company's security solution portfolio. Easy to deploy, manage, and maintain, Acronis XDR expands on the current endpoint detection and response (EDR) offering and delivers complete natively integrated, highly efficient cybersecurity with data protection, endpoint management, and automated recovery specifically built for managed service providers (MSPs).

Cyberattacks have become increasingly sophisticated due to cybercriminals deploying AI and attack surfaces expanding, allowing businesses to be more vulnerable to data breaches and malware. To protect their customers, MSPs who offer security services commonly only have a choice of complex tools with insufficient, incomplete protection that are expensive and time-consuming to deploy and maintain. As a direct response to these challenges, Acronis XDR is the solution providing complete protection without high costs and added complexity.

"Acronis makes a compelling entrance into XDR," notes Chris Kissel, Research Vice-President at IDC. "Acronis has provided an endpoint protection platform for the better part of a year. They have extended their XDR stack mapping alerts to MITRE ATTACK and offer cloud correlation detections. Importantly, their platform supports multitenancy, and the dashboard provides intuitive visualizations."

Key features and benefits of Acronis XDR include:

- Native integration across cybersecurity, data protection, and endpoint management. The product is designed to protect vulnerable attack surfaces enabling unmatched business continuity.
- High efficiency, with the ability to easily launch, manage, scale, and deliver security services. It also includes AI-based incident analysis and single-click response for swift investigation and response.
- Built for MSPs, including a single agent and console for all services, and a customizable platform to integrate additional tools into a unified technology stack.

"It is imperative that MSPs provide reliable cybersecurity to customers with diverse IT environments and constrained budgets," said Gaidar Magdanurov, President at Acronis."Acronis XDR enables MSPs to offer top-notch security without the complexity and significant overhead of traditional non-integrated tools. This is achieved in several ways, including AI-assisted capabilities within the Acronis solution that helps MSPs provide the utmost cybersecurity - even if an MSP only has limited cybersecurity expertise."

KASPERSKY FINDS 24 VULNERABILITIES IN CHINESE BIOMETRIC ACCESS SYSTEMS

Kaspersky has identified numerous flaws in the hybrid biometric terminal produced by international manufacturer ZKTeco. By adding random user data to the database or using a fake QR code, a nefarious actor can easily bypass the verification process and gain unauthorized access. Attackers can also steal and leak biometric data, remotely manipulate devices, and deploy backdoors. High-security facilities worldwide are at risk if they use this vulnerable device.

The flaws were discovered in the course of Kaspersky Security Assessment experts' research into the software and hardware of ZKTeco's white-label devices. All findings were proactively shared with the manufacturer prior to public disclosure.

kaspersky

The biometric readers in question are widely used in areas across diverse sectors – from nuclear or chemical plants to offices and hospitals. These devices support face recognition and QR-code authentication, along with the capacity to store thousands of facial templates. However, the newly discovered vulnerabilities expose them to various attacks. Kaspersky grouped the flaws based on the required patches, and registered them under specific CVEs (Common Vulnerabilities and Exposures).

The CVE-2023-3938 vulnerability allows cybercriminals to perform a cyberattack known as SQL injection, which involves inserting malicious code into strings sent to a terminal's database. Attackers can inject specific data into the QR code used for accessing restricted areas. Consequently, they can gain unauthorized access to the terminal and physically access the restricted areas.

When the terminal processes a request containing this type of malicious QR code, the database mistakenly identifies it as originating from the most recently authorized legitimate user. If the fake QR code contains an excessive amount of malicious data, rather than granting access, the device restarts

DELL TECHNOLOGIES AND ARAMCO TO EXPLORE COLLABORATION OPPORTUNITIES IN EMERGING TECHNOLOGIES

Dell Technologies and Aramco have signed a Memorandum of Understanding (MoU) to explore opportunities in quantum computing, artificial intelligence (AI), edge computing solutions, and advanced computing architectures.

The role of technologies such as AI-enabled edge and quantum computing can help address complex problems in areas such as energy optimization, predictive maintenance, weather modeling, and materials science. The combination of AI and edge computing, along with a robust and scalable enterprise IT infrastructure, is expected to allow businesses to optimize operations, foster real-time data processing, and enhance computational efficiencies.

The MoU underscores Aramco's aim to drive innovation in the global energy sector and paves the way for potential collaborations that could lead to future technological advancements.

Nabil Al Nuaim, Senior Vice President of Digital & Information Technology, Aramco, said: "Technologies such as AI and quantum computing offer unparalleled processing capabilities and could be gamechangers in the energy sector. The potential is limitless, and we are excited to explore new opportunities with Dell. These opportunities could enable us to further align with our sustainability goals and help contribute to the Kingdom's position as a technological frontrunner in the energy domain."

DU TO LAUNCH HYPERSCALE CLOUD AND SOVEREIGN AI SERVICES FOR THE UAE GOVERNMENT WITH ORACLE ALLOY

du, from Emirates Integrated Telecommunications Company (EITC), has announced it will deploy Oracle Alloy to offer hyperscale cloud and sovereign AI services for the government and public sector entities in the UAE focusing on Dubai and the Northern Emirates. The signing ceremony took place during the AI Retreat, a premier gathering held under the patronage of H.H Sheikh Hamdan bin Muhammed bin Rashid Al Maktoum, Crown Prince of Dubai and Chairman of the Executive Council of Dubai, attended by decision makers, industry leaders, AI experts from government and private sectors and global tech giants to discuss strategies, challenges and opportunities presented by AI locally and globally.

Oracle Alloy is a complete cloud infrastructure platform that enables Oracle partners to become cloud providers. With this platform, du can provide more than 100 Oracle Cloud Infrastructure (OCI) services together with its own value-added cloud services and applications. This will enable du to become the first local hyperscale cloud provider to offer a comprehensive set of cloud services branded under its portfolio.

The services will be customized to meet the specific needs of the UAE markets and industry verticals, while ensuring alignment with the UAE regulatory requirements. du will also use Oracle Alloy to accelerate its internal digital transformation strategy and ensure the full modernization of its internal IT and engineering ecosystem.

du will also benefit from Oracle and NVIDIA's collaboration, enabling du to offer sovereign AI capabilities and its new GPU-as-a-Service to government entities in Dubai and Northern Emirates. Oracle's distributed cloud, AI Services, and generative AI services, combined with NVIDIA's accelerated computing platform and software, will enable du to quickly deploy AI capabilities for its public sector customers.

Fahad Al Hassawi, CEO of du said: "The UAE is one of the fastest-growing cloud services markets in the world, and public sector entities in the UAE are rapidly embracing the benefits of the cloud, including added agility, efficiency, security, and access to the latest digital technologies such as AI and machine learning. The deployment of Oracle Alloy is a major step in our evolution into a cloud services market, complementing our wide portfolio of managed services with comprehensive public cloud capabilities that enable us to respond nimbly to the transformation demands of our customers. The ability to deploy AI services in a dedicated cloud region within our local data centre in the UAE is particularly valuable in helping our government customers accelerate their transformation initiatives from a facility within the UAE."

Complexity Impacts Effective Security Eliminate Complexity through Convergence and Consolidation Enabled by the Fortinet Security Fabric

Cybersecurity, everywhere you need it

www.fortinet.com

FORTINET®

THE KEY TO MODERN DAY SECURITY

TO DELVE DEEPER INTO THE SIGNIFICANCE OF IAM AND ITS EVOLVING ROLE IN TODAY'S DIGITAL ECOSYSTEMS, ANITA JOSEPH CAUGHT UP WITH INDUSTRY EXPERT, **ZAEEM QADRI**, BUSINESS UNIT HEAD – IDENTITY & ACCESS MANAGEMENT AT GULF IT. WITH EXTENSIVE EXPERIENCE IN CYBERSECURITY AND IAM IMPLEMENTATION, ZAEEM OFFERS INVALUABLE INSIGHTS INTO THE CHALLENGES, INNOVATIONS, AND FUTURE TRENDS SHAPING THE IAM LANDSCAPE IN THE MIDDLE EAST MARKET.

In the ever-expanding digital landscape, where data is currency and breaches are constant threats, the importance of robust Identity Access Management (IAM) cannot be overstated. IAM encompasses the policies, technologies, and processes that enable the right individuals to access the right resources at the right times for the right reasons. As organizations grapple with the complexities of securing their digital assets, IAM emerges as a crucial component in safeguarding sensitive information and maintaining regulatory compliance.

Can you provide an overview of the current landscape of Identity Access Management in the Middle East market?

The Middle East market is experiencing a rapid digital transformation across various sectors, including government, finance, healthcare, and energy. Organizations are increasingly recognizing the importance of IAM in securing their digital assets and ensuring compliance with regulatory requirements. Identity Access Management, is essentially the framework that governs and manages digital identities within an organization. It encompasses processes, technologies, and policies that ensure the right individuals have appropriate access to resources, while unauthorized individuals are kept out. In today's interconnected and data-driven world, where cyber threats are becoming increasingly sophisticated, IAM serves as the first line of defence in protecting sensitive information, preventing data breaches, and ensuring regulatory compliance.

How has IAM evolved over the years in the Middle East, and what are some of the key developments driving its evolution?
The evolution of IAM in the Middle East, has been remarkable, driven primarily by advancements in technology and shifts in the cybersecurity landscape. Initially, IAM was primarily focused on managing user identities and their access to on-premises resources. However, with the proliferation of cloud computing, mobile devices, and the Internet of Things (IoT), IAM had to adapt to accommodate these new challenges. Today, modern IAM solutions offer seamless integration across hybrid environments, support for multi-factor authentication, and sophisticated analytics for risk-based access controls. Additionally, the emergence of Identity as a Service (IDaaS) and Zero Trust security models are transforming how organizations approach IAM, moving away from traditional perimeter-based security towards a more dynamic and identity-centric approach.

What are some of the common challenges organizations face when implementing IAM solutions, and how can they overcome these challenges?
One of the primary challenges organizations encounter is the complexity of IAM deployments, especially in large and heterogeneous environments. Managing identities across multiple systems, applications, and cloud platforms can be daunting, leading to issues such as identity sprawl, inconsistent access controls, and compliance gaps. To address these challenges, organizations need to take a holistic approach to IAM, starting with comprehensive identity governance strategies, robust identity lifecycle management, and automated provisioning and deprovisioning processes. It's also essential to involve key stakeholders from across the organization, including IT, security, compliance, and business units, to ensure alignment and buy-in throughout the IAM journey.

> THE EVOLUTION OF IAM IN THE MIDDLE EAST HAS BEEN DRIVEN PRIMARILY BY ADVANCEMENTS IN TECHNOLOGY AND SHIFTS IN THE CYBERSECURITY LANDSCAPE.

How do you envision the future of IAM evolving in the Middle East market, and what role will technologies such as artificial intelligence and blockchain play?
In the future, we expect to see increased adoption of AI-driven identity analytics and risk-based access controls, enabling organizations to detect and respond to threats in

real-time. Blockchain technology also holds promise for enhancing identity management, particularly in scenarios where decentralized and tamper-proof identity verification is required. As organizations continue to embrace digital transformation, the demand for CIAM solutions that deliver personalized and secure customer experiences will continue to grow. AI and machine learning will play a crucial role in enabling organizations to leverage customer data to deliver personalized services while ensuring compliance with data privacy regulations.

Thank you for sharing your expertise with us today. Before we conclude, do you have any final thoughts or recommendations for organizations looking to strengthen their IAM strategies?

As organizations in the Middle East embark on their digital transformation journeys, Identity Access Management emerges as a critical enabler of trust, security, and compliance. GULF IT has partnered with leading IAM vendors such as SailPoint (IGA) Ping Identity,(AM & CIAM) and CyberArk (PAM) organizations can strengthen their security posture, protect their digital assets, and deliver seamless and secure experiences to their users and customers.

As organizations navigate the complexities of the digital frontier, Identity Access Management emerges as a critical enabler of trust, security, and compliance in an increasingly interconnected world. By embracing the principles of least privilege, zero trust, and continuous monitoring, organizations can safeguard their digital assets, empower their workforce, and embark on their journey towards a secure and resilient future.

GENETEC ANNOUNCES EXPERIENCE CENTERS TO SUPPORT RAPID GROWTH

Genetec Inc. ("Genetec"), a leading technology provider of unified security, public safety, operations, and business intelligence solutions, announced the opening of several new R&D hubs, Experience Centers, and the expansion of several offices around the world.

New R&D hubs

Underscoring its commitment to innovation, Genetec is expanding its global footprint with the establishment and expansion of new research and development hubs in strategic locations worldwide. Located in Vienna (Austria), Krakow (Poland), and Orléans (France), these R&D centers will complement the company's existing Montréal-based campus and its other R&D centers in Québec City and Sherbrooke (Canada), Paris (France), and Bruges (Belgium).

"These new offices serve as innovation hubs, fostering collaboration amongst our developers as they build the forward-thinking technology that Genetec is known for. Our newest R&D centers will bolster existing initiatives and new capabilities such as intelligent automation," said Christian Morin, Vice President of Product Engineering, Genetec Inc. "Not surprisingly, to meet the growing demand for Genetec innovation, we've grown our R&D team by 50% in the past five years."

New Experience Centers and office expansions

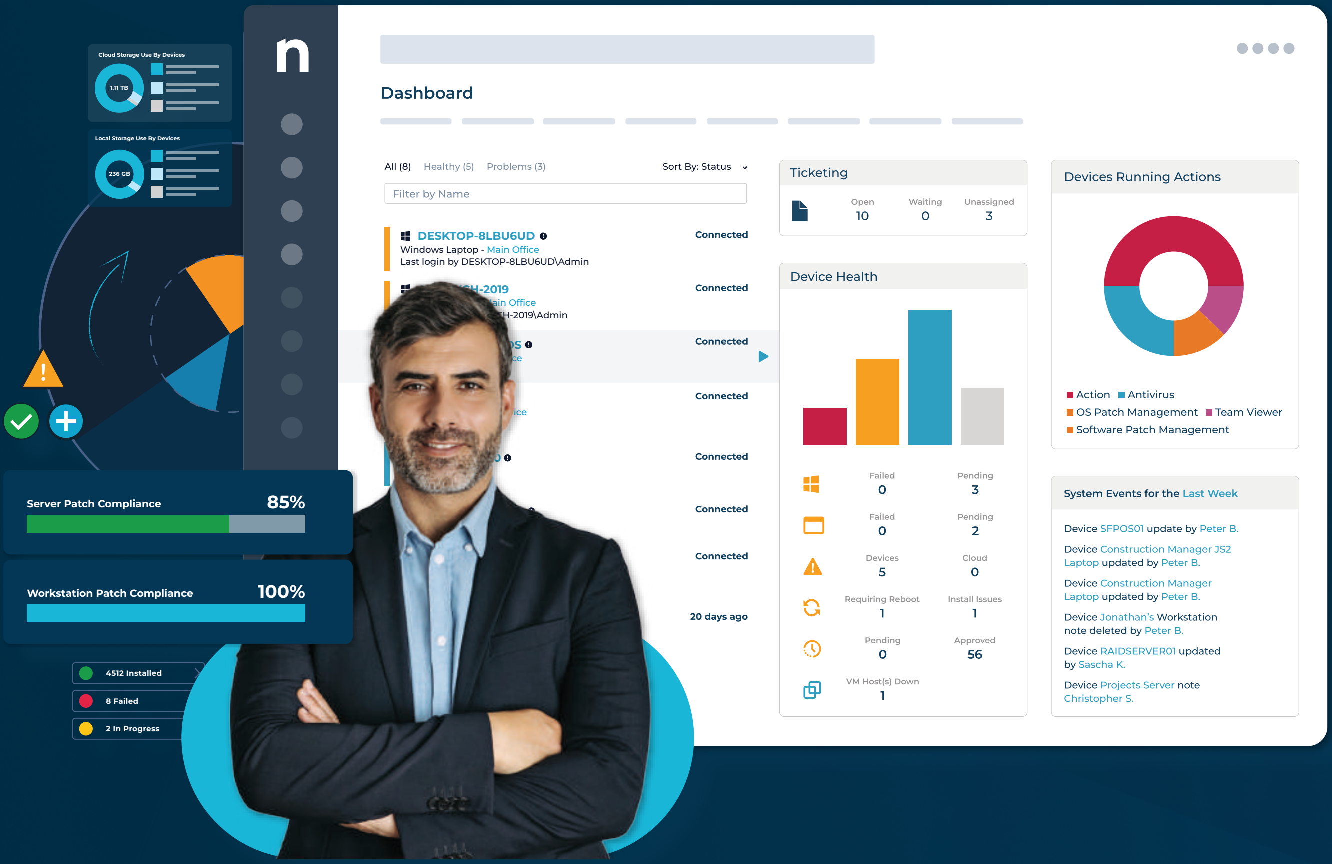
Genetec has also recently opened three new state-of-the-art Experience Centers in Washington D.C. (USA), Sydney (Australia), and Dubai (UAE), in addition to its existing flagship Experience Centers in Montréal (Canada), Paris (France), the City of London (UK), Singapore, and Mexico City (Mexico). Genetec also continues to grow its Montréal headquarters campus, recently adding over 100,000 square feet – including two subsidized bistros for its Montréal-based employees. The company has also significantly expanded its offices in London, Paris, Vienna, and São Paulo (Brazil).

"By launching new experience centers and offices in these strategic locations, we're not just expanding our global presence; we're scaling to meet the increasing demand for Genetec solutions across the globe. Our goal is to provide customers, channel partners, and prospects a hands-on encounter with our innovative technology, and an unforgettable brand experience," said Michel Chalouhi, Vice President of Global Sales, Genetec Inc.

Since 2020, the company has grown its total headcount by 52% and currently has over 2,100 employees located in 20 offices across four continents. As part of its ongoing efforts to accommodate its organic growth, the company is currently recruiting to fill over 80 new positions, including over 30 openings in R&D across the Americas, Europe, the Middle East, and Asia Pacific regions.

ninjaOne

The Unified IT Management Platform



Cloud Storage Use By Devices

1.11 TB

Local Storage Use By Devices

236 GB

Dashboard

All (8) Healthy (5) Problems (3) Sort By: Status

Filter by Name

DESKTOP-8LBU6UD
Windows Laptop - Main Office
Last login by DESKTOP-8LBU6UD\Admin
Connected

H-2019
ain Office
H-2019\Admin
Connected

S
ce
Connected

ice
Connected

O
Connected

Connected

Connected

20 days ago

Ticketing

Open	Waiting	Unassigned
10	0	3

Device Health

⊞	Failed 0	Pending 3
▭	Failed 0	Pending 2
⚠	Devices 5	Cloud 0
⟳	Requiring Reboot 1	Install Issues 1
◷	Pending 0	Approved 56
⧉	VM Host(s) Down 1	

Devices Running Actions

■ Action ■ Antivirus
■ OS Patch Management ■ Team Viewer
■ Software Patch Management

System Events for the Last Week

Device SFPOS01 update by Peter B.

Device Construction Manager JS2 Laptop updated by Peter B.

Device Construction Manager Laptop updated by Peter B.

Device Jonathan's Workstation note deleted by Peter B.

Device RAIDSERVER01 updated by Sascha K.

Device Projects Server note Christopher S.

Server Patch Compliance 85%

Workstation Patch Compliance 100%

● 4512 Installed
● 8 Failed
● 2 In Progress

Manage, Patch and Support All your Endpoints

- ✓ Unify and automate device management
- ✓ Get 360° visibility and control
- ✓ Patch and support any device anywhere
- ✓ Free onboarding, free training, free support
- ✓ Quick to deploy, easy-to-use, with a single intuitive UI

ninjaone.com

LEARN MORE

UNVEILING THE KEY FINDINGS OF THE SANS INSTITUTE 2024 CYBER THREAT INTELLIGENCE SURVEY

SANS Institute, a global leader in cybersecurity training, has published the 2024 Cyber Threat Intelligence (CTI) Survey, authored by renowned cybersecurity experts, SANS Certified Instructor Rebekah Brown and SANS Instructor Candidate Andreas Sfakianakis. With a dramatic rise in covert activities, cloud breaches, and AI-driven attacks, the insights from this survey are vital for CISOs, CIOs, and security professionals looking to stay ahead of adversaries. Understanding the latest trends and preparing for emerging threats can help organizations protect their digital assets and maintain trust with customers and stakeholders.

As cyber threats continue to evolve in complexity and sophistication, this year's survey highlights pivotal insights that are essential for organizations aiming to bolster their defenses with groundbreaking insights into the evolving threat landscape, with a focus on the significant influence of geopolitical events, the burgeoning role of artificial intelligence, and the emerging dominance of threat hunting within CTI teams.

Geopolitical and Regulatory Influences

Geopolitics and new regulations are profoundly shaping CTI team activities. "The increasing frequency and complexity of global conflicts have made it essential for CTI teams to broaden their focus beyond internal issues," said Brown. "Our survey shows that 77.5% of respondents recognize the significant impact of geopolitics on their intelligence requirements, highlighting the need for adaptive and informed responses to external threats." Additionally, 74% of respondents emphasize the importance of adapting to new regulations, underscoring the necessity for CTI teams to stay compliant with evolving legal landscapes.

Rise of Threat Hunting

For the first time, threat hunting has emerged as the top use case for CTI. This proactive approach to detecting unidentified threats has seen substantial reliance on the MITRE ATT&CK framework, with over 95% of respondents utilizing it for categorizing and communicating tactics, techniques, and procedures (TTPs). "The prominence of threat hunting reflects a strategic shift in how organizations are leveraging CTI," Sfakianakis noted. "This approach not only enhances detection capabilities but also strengthens overall security posture."

Impact of Artificial Intelligence

AI is making significant inroads in CTI, with nearly one-quarter of respondents already leveraging AI in their programs and another 38% planning to adopt it. "Artificial intelligence is becoming a crucial tool for CTI teams, helping analysts prioritize and process vast amounts of information through advanced scoring and summarization techniques," said Brown. However, she also highlighted the growing concern about the adversarial use of AI, stressing the importance of preparing for AI-driven threats.

Integration via Threat Intelligence Platforms (TIPs)

The survey highlights the critical role of Threat Intelligence Platforms (TIPs) in integrating CTI into the security stack. A notable 58% of participants reported incorporating CTI into their detection and response controls through TIPs' built-in integration capabilities. "The mature state of TIPs demonstrates their effectiveness in disseminating threat intelligence across security tools, enhancing the overall efficiency of CTI programs," Sfakianakis explained.

THIS YEAR'S SURVEY HIGHLIGHTS PIVOTAL INSIGHTS THAT ARE ESSENTIAL FOR ORGANIZATIONS AIMING TO BOLSTER THEIR DEFENSES WITH GROUNDBREAKING INSIGHTS INTO THE EVOLVING THREAT LANDSCAPE.

CTI in Vulnerability Management

The role of CTI in vulnerability management has seen a significant increase, with 66% of respondents now using CTI to pinpoint actively exploited vulnerabilities. This marks a rise from 54% in 2017, demonstrating CTI's pivotal role in prioritizing patches and supporting vulnerability remediation efforts. "Our findings highlight the growing reliance on CTI for operational purposes in vulnerability management, with 83% of respondents considering it essential for identifying and addressing critical vulnerabilities," Brown stated.

THE TRUST FACTOR

SECURITY ADVISOR MIDDLE EAST EXAMINES THE INCREASING RELEVANCE OF THE ZERO TRUST APPROACH IN BUILDING A ROBUST DEFENSE AGAINST ADVANCED CYBERTHREATS.

THE ZERO TRUST MODEL OPERATES ON A FOUNDATIONAL PRINCIPLE: NEVER TRUST, ALWAYS VERIFY.

In an era where cyber threats are evolving at an unprecedented rate, traditional security models are struggling to keep pace. Organizations across the globe are realizing that the old mantra of "trust but verify" is no longer sufficient in the face of sophisticated cyber-attacks. Enter the Zero Trust approach to cybersecurity—a paradigm shift that promises to fortify defenses in today's digitally-driven world.

The Essence of Zero Trust

The Zero Trust model operates on a foundational principle: never trust, always verify. Unlike conventional security strategies that assume entities inside an organization's network are trustworthy, Zero Trust assumes that threats could come from both inside and outside the network. Therefore, no entity—be it user, device, or system—is trusted by default. Instead, every access request is meticulously authenticated, authorized, and encrypted before any connection is made.

This shift is critical. With the proliferation of cloud computing, mobile devices, and remote work, the network perimeter has become increasingly porous. Traditional security measures, which focus primarily on defending the perimeter, are rendered inadequate in this new landscape. Zero Trust addresses these vulnerabilities by eliminating implicit trust and ensuring that security is maintained continuously, regardless of where access requests originate.

Key Components of the Zero Trust Framework

Implementing a Zero Trust architecture involves several core components, each playing a pivotal role in creating a resilient cybersecurity posture:

1. **Identity and Access Management (IAM):** Central to Zero Trust is the need to verify every user and device. IAM solutions ensure that only authorized individuals and systems can access sensitive data and resources. This involves multi-factor authentication (MFA), single sign-on (SSO), and continuous monitoring of user behavior.

2. **Least Privilege Access:** Zero Trust enforces the principle of least privilege, granting users and devices the minimal level of access necessary to perform their functions. This reduces the attack surface and limits the potential damage from compromised accounts.

3. **Microsegmentation:** This technique involves dividing the network into smaller, isolated segments to prevent lateral movement by attackers. Even if a breach occurs in one segment, it cannot easily spread

to others, containing the potential impact.

4. **Continuous Monitoring and Threat Detection:** Zero Trust relies on real-time monitoring of all network traffic and user behavior. Advanced analytics and machine learning are used to detect anomalies and potential threats, enabling swift response and mitigation.

5. **Encryption:** All data, whether at rest or in transit, is encrypted to protect it from interception and tampering. This ensures that even if data is accessed by unauthorized entities, it remains unintelligible.

Benefits of Zero Trust

Adopting a Zero Trust model brings a multitude of benefits to organizations:

1. **Enhanced Security:** By removing implicit trust and enforcing strict verification, Zero Trust significantly reduces the risk of data breaches and unauthorized access. It ensures that even if attackers penetrate the network, their ability to cause harm is severely limited.

2. **Improved Compliance:** Zero Trust architectures are inherently aligned with regulatory requirements for data protection and privacy. They provide detailed logs and audit trails, facilitating easier compliance with standards such as GDPR, HIPAA, and CCPA.

ZERO TRUST ARCHITECTURES ARE INHERENTLY ALIGNED WITH REGULATORY REQUIREMENTS FOR DATA PROTECTION AND PRIVACY.

3. **Operational Efficiency:** While Zero Trust may seem resource-intensive initially, it ultimately streamlines security operations. Automated processes for authentication and access management reduce the burden on IT staff, allowing them to focus on more strategic initiatives.

4. **Resilience Against Evolving Threats:** Cyber threats are constantly evolving, with attackers developing new techniques to bypass defenses. Zero Trust's adaptive and continuous verification processes ensure that organizations remain resilient against both current and emerging threats.

Challenges and Considerations

Despite its advantages, transitioning to a Zero Trust model presents several challenges:

1. **Complexity:** Implementing Zero Trust requires a comprehensive overhaul of existing security

frameworks. Organizations must invest in new technologies, integrate disparate systems, and retrain staff, all of which can be complex and costly.

2. **Cultural Shift:** Zero Trust necessitates a cultural change within organizations. Employees must adapt to new security protocols, which can initially be met with resistance. Effective communication and training are crucial to gaining buy-in from all stakeholders.

> ZERO TRUST OFFERS A REVOLUTIONARY APPROACH THAT ALIGNS WITH THE REALITIES OF TODAY'S DIGITAL LANDSCAPE.

3. **Scalability:** Ensuring that Zero Trust principles are scalable across large, distributed networks can be challenging. Organizations need robust solutions capable of handling high volumes of authentication and monitoring without compromising performance.

The Future of Cybersecurity

As cyber threats continue to escalate, the need for a robust, adaptive security model becomes increasingly evident. Zero Trust offers a revolutionary approach that aligns with the realities of today's digital landscape. By eliminating implicit trust and enforcing stringent verification processes, Zero Trust not only enhances security but also builds a resilient defense against future threats.

> ZERO TRUST NOT ONLY ENHANCES SECURITY BUT ALSO BUILDS A RESILIENT DEFENSE AGAINST FUTURE THREATS.

Organizations willing to embrace this paradigm shift will find themselves better equipped to protect their critical assets and maintain the trust of their customers and stakeholders. The journey to Zero Trust may be challenging, but the rewards—a secure, resilient, and compliant cybersecurity posture—are well worth the effort. In an uncertain cyber world, Zero Trust stands as a beacon of security and reliability.

SOPHOS UNCOVERS CHINESE ESPIONAGE CAMPAIGN IN SOUTHEAST ASIA

Sophos, a global leader of innovative security solutions for defeating cyberattacks, has released its report, "Operation Crimson Palace: Threat Hunting Unveils Multiple Clusters of Chinese State-Sponsored Activity Targeting Southeast Asia," which details a highly sophisticated, nearly two-year long espionage campaign against a high-level government target. During Sophos X-Ops' investigation, which began in 2023, the managed detection and response (MDR) team found three distinct clusters of activity targeting the same organization, two of which included tactics, techniques and procedures (TTPs) that overlap with well-known, Chinese nation-state groups: BackdoorDiplomacy, APT15 and the APT41 subgroup Earth Longzhi.

The attackers designed their operation to gather reconnaissance on specific users as well as sensitive political, economic, and military information, using a wide variety of malware and tools throughout the campaign that Sophos has since dubbed "Crimson Palace." This includes previously unseen malware: a persistence tool that Sophos named PocoProxy.

"The different clusters appear to have been working in support of Chinese state interests by gathering military and economic intelligence related to the country's strategies in the South China Sea. In this particular campaign, we believe these three clusters represent distinct groups of attacks who are working in parallel against the same target under the overarching directive of a central state authority. Within just one of the three clusters that we identified—Cluster Alpha— we saw malware and TTPs overlap with four separately reported Chinese threat groups. It's well-known that Chinese attackers share infrastructure and tooling, and this recent campaign is a reminder of just how extensively these groups share their tools and techniques.

"As Western governments elevate awareness about cyberthreats from China, the overlap Sophos has uncovered is an important reminder that focusing too much on any single Chinese attribution may put organizations at risk of missing trends about how these groups coordinate their operations," said Paul Jaramillo, director, threat hunting and threat intelligence, Sophos. "By having the bigger, broader picture, organizations can be smarter about their defenses."

Cluster Alpha was active from early March to at least August 2023 and deployed a variety of malware focused on disabling AV protections, escalating privileges and conducting reconnaissance. This included an upgraded version of the EAGERBEE malware that has been associated with the Chinese threat group REF5961. Cluster Alpha also utilized TTPs and malware that overlap with the Chinese threat groups BackdoorDiplomacy, APT15, Worok, and TA428.

Cluster Bravo was only active in the targeted network for a three-week span in March 2023 and focused on moving laterally through the victim's network to sideload a backdoor called CCoreDoor. This backdoor establishes external communications pathways for the attackers, performs discovery and exfiltrates credentials.

Cluster Charlie was active from March 2023 to at least April 2024, with a focus on espionage and exfiltration. This included the deployment of PocoProxy: a persistence tool that masquerades as a Microsoft executable and establishes communications with the attackers' command and control infrastructure. Cluster Charlie worked to exfiltrate a large volume of sensitive data for espionage purposes, including military and political documents and credentials/tokens for further access within the network. Cluster Charlie shares TTPs with Chinese threat group Earth Longzhi, a reported subgroup of APT41. Unlike Cluster Alpha and Cluster Bravo, Cluster Charlie remains active.

"What we've seen with this campaign is the aggressive development of cyberespionage operations in the South China Sea. We have multiple threat groups, likely with unlimited resources, targeting the same high-level government organization for weeks or months at a time, and they are using advanced custom malware intertwined with publicly available tools. They were, and are still, able to move throughout an organization at will, rotating their tools on a frequent basis. At least one of the activity clusters is still very much active and attempting to conduct further surveillance.

"Given how often these Chinese threat groups overlap and share tooling, it's possible that the TTPs and novel malware we observed in this campaign will resurface in other Chinese operations globally. We will keep the intelligence community informed of what we find as we continue our investigations into these three clusters," Jaramillo said.

THE ATTACKERS DESIGNED THEIR OPERATION TO GATHER RECONNAISSANCE ON SPECIFIC USERS AS WELL AS SENSITIVE POLITICAL, ECONOMIC, AND MILITARY INFORMATION.

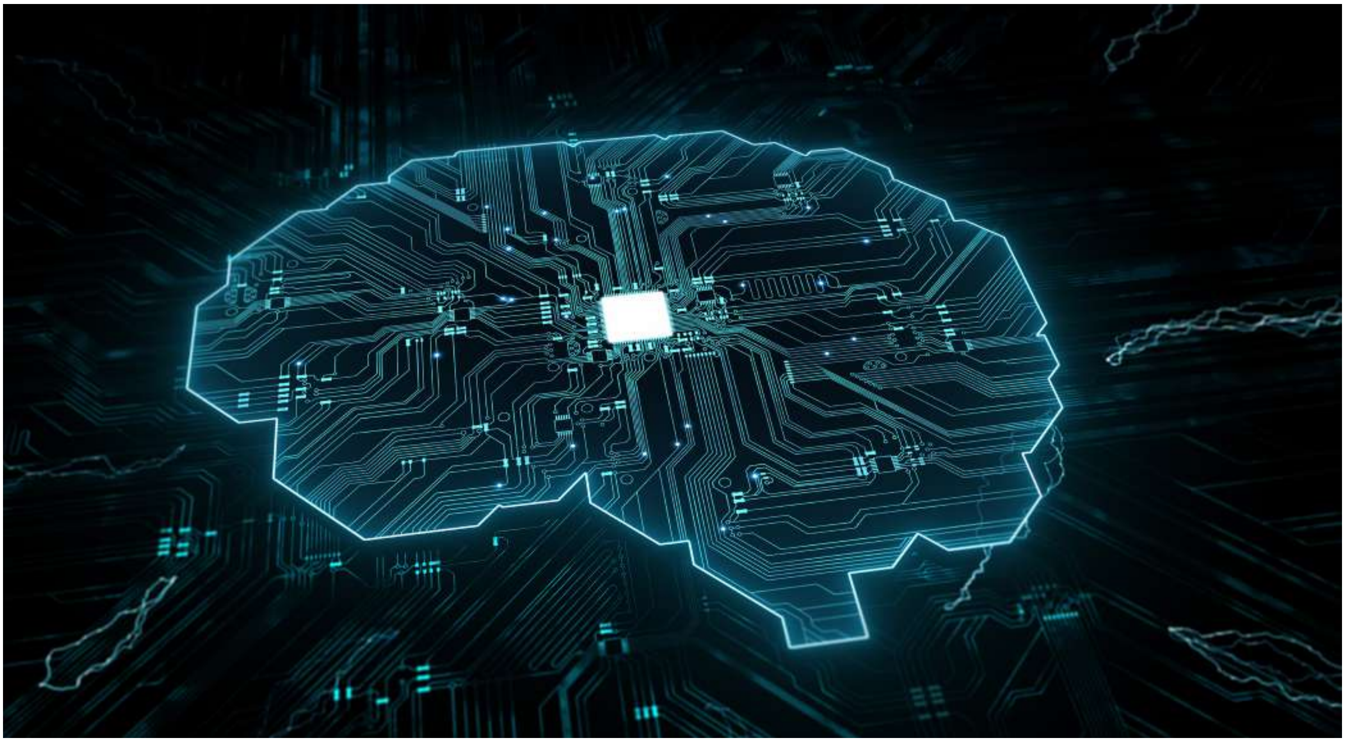
AI-POWERED SECURITY

AHMAD HALABI, MANAGING DIRECTOR AT RESECURITY, IS A HALL-OF-FAME HACKER AND A WIDELY RECOGNIZED VULNERABILITY AND OFFENSIVE CYBERSECURITY RESEARCHER WHO DISCOVERED OVER 2,000 VULNERABILITIES AND HELPED SECURE OVER 200 PRIVATE, PUBLIC AND GOVERNMENT ORGANIZATIONS WORLDWIDE. HALABI IS ALSO A WELL-KNOWN THOUGHT LEADER IN THE PENETRATION TESTING AND BUG BOUNTY FIELD, RANKING AS ONE OF THE TOP 50 HACKERS IN THE WORLD AND TOP ETHICAL HACKER BY THE U.S. DEPARTMENT OF DEFENSE (DOD) AND IBM.

IN AN EXCLUSIVE INTERVIEW WITH SECURITY ADVISOR, HALABI TELLS ANITA JOSEPH HOW RESECURITY COMBINES THE BEST OF HUMAN AND ARTIFICIAL INTELLIGENCE TO OFFER A COMPREHENSIVE, HOLISTIC APPROACH TO SECURITY THAT HELPS BUSINESSES STAY AHEAD OF THE MOST ADVANCED CYBER THREATS.

What is Resecurity's focus in this region, particularly for 2024?
Resecurity is a cybersecurity intelligence firm specializing in threat intelligence-driven solutions. These solutions help mitigate both direct and indirect threats. Our vision for 2024, consistent with previous years, is to reduce cyber threats to the maximum extent possible. We aim to enable enterprises, individuals and even governments to protect themselves against emerging threats targeting them or their perimeters.

Let's talk about the current cyber threat landscape, particularly in this region. What trends and patterns are you seeing?
Threat actors are continually developing new techniques, especially leveraging AI to their advantage. Just as cybersecurity companies use AI for defense, threat actors use it to bypass security controls. The increasing threat landscape is primarily due to human error and lack of awareness. Many rely too heavily on vendors and tools without fully understanding how to use them properly, leaving configurations vulnerable. The key issue is human error and lack of awareness. We need to focus on educating people about the evolving nature of cybersecurity and threats, ensuring a balanced and comprehensive defense to mitigate these threats effectively.



Let's delve into AI and emerging technologies. How do you think AI is helping businesses develop robust cyber defense strategies?
AI is extremely beneficial in predicting and preventing cyber-attacks. However, AI alone isn't enough; it needs to work in tandem with human intelligence. While AI can process vast amounts of data to predict threats, it requires human oversight to provide optimal mitigation. At our company, we've built large datasets and integrated them with our AI model to predict, prevent, and monitor cyber threats. We analyze threat actors' motives, behaviors, tactics, and methodologies to anticipate their next moves before they occur. This combination of AI and human intelligence allows us to identify potential breaches early, providing a significant advantage.

Does your company have any unique solutions that set it apart in the cybersecurity market?
Yes, imagine using AI as a weapon to counteract threats targeting you. We are developing an AI model that can provide comprehensive information about any threat targeting you, including indicators of compromise, tools, techniques, and procedures. Our AI can search over 30,000 sources, including dark web channels, to determine if you are being targeted or if there has been a material breach. For instance, you could ask our AI if a specific individual is compromised, and it would scan the entire internet to provide an answer within seconds. This capability can save a lot of time, resources and money by simplifying the threat detection process.

In your experience, what are some of the challenges businesses in this region face, and what attack trends should they be prepared for?
The challenges aren't only cyber-related but also physical. The rapid growth in this region means scalability is a major issue. Companies often lack visibility over all their assets, which can give threat actors an advantage. Another significant challenge is the lack of awareness and education among employees. Many organizations invest heavily in security products but don't educate their employees on proper usage. Human error, such as downloading malicious software while working remotely, can compromise company security. It's crucial to educate employees about cybersecurity, not just within the work environment but also in their personal lives, as threat actors often target personal devices to infiltrate corporate networks.

Tell us how Resecurity is reshaping the identity protection landscape.
Protecting employees' identities is crucial because you can't monitor their personal devices. We offer identity protection services that allow individuals to detect if their personal information is leaked or compromised. This includes monitoring emails, phone numbers, credit cards, social media accounts, and more. By protecting personal information, we prevent minor threats from escalating into major ones. Our comprehensive approach includes monitoring not just the company's assets but also its surroundings, including third-party vendors and suppliers, to ensure complete security.

At Resecurity, we are committed to protecting everyone—whether an individual, a large organization, or a government—from any cyber threat. We monitor all aspects of cybersecurity, addressing both major and minor threats to ensure comprehensive protection.

RUCKUS
COMMSCOPE

PURPOSE-DRIVEN ENTERPRISE NETWORKS

REDEFINING CONNECTIVITY

We live in an ever-growing digital transformation, imposing more challenges on organizations of different sizes to keep pace with technological evolution as well as with the growing demands of citizens, employees, students and guests for seamless, faster and more secure connections.

RUCKUS builds world-class wired & wireless networks that deliver reliable user experience, our patented technologies and AI Engine helps you better drive the transformation whether in small or even in high-dense and tough environments.

EXPLORE OUR PORTFOLIO

SCAN ME

RANSOMWARE VICTIMS UNABLE TO RECOVER 43% OF AFFECTED DATA: VEEAM

Ransomware remains an ongoing threat for organizations and is the largest single cause of IT outages and downtimeas 41% of data is compromised during a cyberattack, according to the latest Veeam 2024 Ransomware Trends Report. The report reveals that only 57% of the compromised data will be recovered, leaving organizations vulnerable to substantial data loss and negative business impact as a result.

"Ransomware is endemic, impacting 3 out of 4 organizations in 2023. AI is now enabling the creation of smarter, more advanced security, but it's also facilitating growth in the volume of sophistication of attacks," said Dave Russell, Senior Vice President, Head of Strategy at Veeam. "Our report delivers a clear message: ransomware attacks will continue, be more severe than predicted, and the overall impact will cost organizations more than they expect. Organizations must take action to ensure cyber resiliency and acknowledge that rapid, clean recovery matters most. By aligning teams and bolstering cybersecurity with immutable backups, they can protect their valuable business data while Veeam keeps their business running and secure."

The third annual Veeam 2024 Ransomware Trends Report draws insights from vetted organizations that experienced at least one successful cyberattack in the preceding 12 months. With 1,200 responses analyzed, comprising executives, information security professionals, and backup administrators, the report provides a comprehensive overview of the evolving threat landscape.

The toll on the organization's people

The report shows that the human impact of cyberattacks cannot be overstated. 45% of surveyed individuals cited increased workload post-attack, while 40% reported heightened stress levels and other personal challenges that are difficult to mitigate on 'normal' days. These challenges, coupled with existing organizational struggles, further underscore the importance of effective cyber defense strategies.

Organizations are misaligned for preparedness

Despite increased focus on cyber-preparedness, organizations still face a misalignment between their backup and cyber teams. For the third consecutive year, close to two-thirds (63%) of organizations find their backup and cyber teams lacking synchronization. Adding to the misalignment challenges in organizations, 61% of security professionals and 75% of backup admins believe that the teams need either 'significant improvement' or that a complete system overhaul is required.

Unveiling the true financial impact

Contrary to the belief that having cyber insurance increases the likelihood of ransom payments, Veeam's research indicates otherwise. Despite only a minority of organizations possessing a policy to pay, 81% opted to do so. Interestingly, 65% paid with insurance and another 21% had insurance but chose to pay without making a claim. This implies that in 2023, 86% of organizations had insurance coverage that could have been utilized for a cyber event.

CYBER-ATTACKS NATURALLY AFFECT AN ORGANIZATION'S FINANCIAL STABILITY, BUT JUST AS SIGNIFICANT IS THE TOLL IT HAS ON TEAMS AND INDIVIDUALS.

Relying on a "good backup"

- The most common component of a cyber preparedness playbook is a "good backup." While cyber and backup teams may not always be organizationally aligned, when asked about the existence of an incident response team (IRT) and whether that team had a playbook, a mere 2% of organizations lacked a pre-identified team. Additionally, only 3% had teams but without a playbook in place.
- Other key findings from the Veeam 2024 Ransomware Trends Report include:
- Cloud and on-premises data are just as easily attackable: Surprisingly, there was no significant variation between how much data was affected within the data center vs. data within remote offices/branch offices or even on data hosted in a public or private cloud. Meaning that all IT infrastructure is just as seamlessly available to the attacker as it is easily accessible to the users.
- Most organizations risk reintroducing infections: Alarmingly, almost two-thirds (63%) of organizations are at risk of reintroducing infections while recovering from ransomware attacks or significant IT disasters. Pressured to restore IT operations quickly and influenced by executives, many organizations skip vital steps, such as rescanning data in quarantine, causing the likelihood of IT teams to inadvertently restore infected data or malware.
- Organizations must ensure recoverable data: As a 'lesson learned', respondents of prior cyberattacks now recognize the importance of immutability with 75% of organizations now utilizing on-premises disks that can be hardened and 85% are utilizing cloud-storage with immutability capabilities. In fact, half of their overall backup storage is immutable, highlighting good improvements but with more work to be done.

SECURING CRITICAL ENVIRONMENTS: OPSWAT'S ZERO TRUST ROUNDTABLE

MetaDefender Core
Advanced Threat Prevention Platform
OPSWAT
A Zero Trust Approach to Protecting Critical Environments

OPSWAT, a global leader in perimeter defense cybersecurity and pioneer of Deep CDR technology, hosted an incisive roundtable recently, on the topic "A Zero Trust Approach to Protecting Critical Environments." The event, dedicated to enhancing the security of critical infrastructures, drew a diverse group of C-level executives, industry experts, and cybersecurity professionals, all eager to delve into OPSWAT's pioneering strategies for a secure digital future.

The session began with a brief yet impactful introduction that set the stage for the discussion. Participants were welcomed to a dynamic exploration of the pressing challenges faced in safeguarding critical sectors, from utilities to healthcare and beyond. The introduction underscored the increasing complexity of cyber threats and the imperative for robust defense mechanisms.

Understanding Critical Infrastructure Challenges

The roundtable, addressed by Rami Nehme, Regional Sales Director - South Gulf, Levant & Pakistan at OPSWAT and Saif AlRefai, Sales Engineering Team Lead – META at OPSWAT, focused on the unique challenges faced by C-level executives in securing critical infrastructures. Infrastructure protection networks are complex and the challenges most organisations face when attempting to implement them are the network

complexity regulation issues, the technology gaps a company may possess after relying on a single antivirus engine for so long and the training gaps caused by a lack of formal critical infrastructure protection certification and training. For each of these problems, they said, OPSWAT has a bespoke solution with its unified platform integrated by design that can overcome complexity and cover any technology gap.

OPSWAT's Unified Zero Trust Approach

Central to the roundtable was OPSWAT's revolutionary unified Zero Trust approach tailored for critical environments. This approach operates on the principle of "never trust, always verify," ensuring that every user and device accessing the network is authenticated and continuously validated. The event provided a deep dive into how this methodology is particularly suited to critical infrastructures, where the stakes are exceptionally high. OPSWAT's solution encompasses endpoint security, network security, and continuous monitoring, offering a robust framework to defend against sophisticated cyber threats.

> OPSWAT'S REVOLUTIONARY UNIFIED ZERO TRUST APPROACH OPERATES ON THE PRINCIPLE OF "NEVER TRUST, ALWAYS VERIFY," ENSURING THAT EVERY USER AND DEVICE ACCESSING THE NETWORK IS AUTHENTICATED AND CONTINUOUSLY VALIDATED.

Rami and Saif elaborated on how the key principles of Zero Trust can be represented with the five pillars of the CISA Maturity Model. The five pillars consist of Identity, Devices, Networks, Applications/Workloads and Data. Identity represents continuous validation and risk analysis, Devices support a continuous physical and virtual asset presence, Networks are used to integrate the best practices for cryptographic agility, Applications/Workloads highlight how vital protections against sophisticated attacks in all workflows are, and Data can be strengthened to provide automated categorization and labelling enterprise-wide.

They also outlined the core elements of OPSWAT's advanced threat prevention platform- MetaDefender, which comprises several vital features that are essential for threat prevention and zero-trust security. Firstly, it exhibits a Deep CDR used to disarm active embedded threats and reconstruct every file to prevent zero-day attacks and advanced evasive malware. With its advanced capabilities multi-scanning can be used to provide a simultaneous analysis with 30+ leading anti-malware engines to detect nearly 100% of known threats. It's proactive DLP can check for sensitive and confidential file content to prevent data leakage and meet regulatory compliance. The inherent file-based vulnerability assessment constantly scans and analyses binaries and installers to detect vulnerabilities before exposure. Finally, it can supply volumes of threat intelligence data to provide enriched insights on threats on billions of hashes, IPs and domains.

Real-World Impact

Illustrating the efficacy of their Zero Trust approach, the OPSWAT spokespersons also shared compelling success stories. One notable example involved a major utility company that faced persistent cyber threats targeting its operational technology (OT) network. By implementing OPSWAT's solutions, the company not only thwarted potential breaches but also achieved enhanced visibility and control over its OT environment. Another success story featured a healthcare provider that significantly reduced its vulnerability to ransomware attacks, safeguarding sensitive patient data and ensuring uninterrupted service delivery.

Cloud
File-based Vulnerability Assessment – Scan and a… …aries and installers to detect vulnerabilities before exposu…
Next-Gen Sandbox – Adaptive threat analysis
Threat Intelligence – Provide enriched intelligence … …n billions of hashes, IPs and domains

Empowering Informed Decision-Making

The session was particularly valuable for decision-makers, equipping them with the knowledge to make informed choices regarding their cybersecurity strategies. The insights provided into the evolving threat landscape and the demonstrated effectiveness of Zero Trust principles allowed attendees to re-evaluate and strengthen their current security postures.

Enhancing Organizational Preparedness

Beyond understanding and strategy, the roundtable emphasized practical preparedness. Attendees left with actionable insights and best practices that could be immediately applied within their organizations. By adopting OPSWAT's unified approach, organizations can better anticipate and respond to threats, thereby enhancing their resilience and readiness.

→ Cloud / Software / Hardware
→ Integrated by Design
Infrastructure Protection
→ Deep Content Disarm & Reconstruction – Zero Trus
→ Multi Engine Antivirus Scanning
→ Next-Gen Sandbox

Engagement with Industry Experts

The interactive segment of the event fostered a rich exchange of ideas and experiences, offering a deeper dive into contemporary security strategies. It also provided a unique networking opportunity, encouraging future collaborations and information sharing among participants.

OPSWAT's roundtable was a critical touchpoint for those tasked with protecting vital infrastructures. Through comprehensive discussions and real-world examples, attendees gained invaluable insights into the challenges and solutions in the cybersecurity landscape. The event underscored OPSWAT's commitment to pioneering effective defense mechanisms and empowering organizations to safeguard their critical environments against ever-evolving threats.

GRC AND SECURITY

ANOOP KUMAR, HEAD OF INFORMATION SECURITY GOVERNANCE RISK AND COMPLIANCE AT AL NISR PUBLISHING, GULF NEWS, TELLS SECURITY ADVISOR ABOUT THE IMPORTANCE OF GRC IN IMPROVING OVERALL SECURITY POSTURE.

How does the governance component of GRC contribute to achieving information security goals within an organization? Can you provide examples of effective governance practices?

Governance primarily defines the roles and responsibilities of business leaders and the policies they create and enforce, it affects every level of the organization. It is a collection of administrative and technical controls with adequate awareness programs built-in to ensure that the required compliance is achieved with adequate Risk Management practices.

Employees across the business should understand the organization's governance components and the role they play in maintaining business operations in a sustainable way ensuring reduced operational risk, reduced cost, and improved performance and achieve desired compliance.

In the context of GRC, what are the key steps involved in identifying and mitigating risks to information security? How does a risk-based approach improve overall security posture?

The importance of GRC extends beyond mere regulatory adherence, playing a vital role in safeguarding sensitive information and fortifying the resilience of organizations against potential cyberattacks. By fostering a culture of proactive risk management and compliance, GRC helps businesses identify vulnerabilities, mitigate risks, and adapt to new threats as they emerge. This strategic approach is crucial in an era where cyber threats are not only increasing in frequency but also in sophistication, targeting the very core of organizational operations.

In Information Security / cybersecurity, Governance, Risk Management, and Compliance (GRC) stands as a fundamental framework, guiding organizations in the implementation of robust security measures. GRC integrates the critical elements of governance, risk management, and compliance to establish a comprehensive approach to cybersecurity. This framework not only addresses the technological aspects but also ensures that organizational practices align with the evolving landscape of cyber threats and regulatory requirements. Risk Assessment and Management must be practiced in all phases of a project, operations and even in change and release management. This approach will enhance Governance, adequate Compliance and ensure all identified Risks mitigated instantly in an iterative mode. Basically, a GRC by design protect, safeguard and ensure information system sustainability of any organization.

Compliance is a critical part of GRC. How do organizations ensure they meet regulatory requirements without compromising their information security goals? Can you share any challenges and solutions you've encountered?

In cybersecurity, compliance refers to the process of adhering to established laws, regulations, standards and organization's internal policies designed to protect data and ensure privacy by a stringent risk management mandates. This critical aspect of cybersecurity focuses on ensuring that organizations meet the required security measures to safeguard sensitive information from unauthorized access, data breaches, and other cyber threats. Compliance is not just about following rules; it's about establishing a culture of security and trust that protects individuals' rights and organizations' integrity.

I must say, GRC itself is very challenging to implement in any organization, as people might think you are stepping on their toes until you comfortably educate them on how to operate GRC, what are their roles and responsibilities, what is in it for them and how organization is going to benefit out it.

How can organizations effectively integrate GRC processes into their existing information security frameworks? What are some best practices for seamless implementation and avoiding common pitfalls?

It is not simple at all, it is all about education and awareness first by adapting and integrating frameworks with defined Process steps, Policies and KPIs. Eg: project management, audit and IT operational frameworks, namely PMP,PMI, Scrum / Agile, COBIT and ITIL

Its like social technical environment creation, bring everyone's culture, Strategy, Tactical and Technology together. Form a Virtual GRC team and agree on process / pipeline by walking through all involved business and administrative processes, namely IT, Finance, legal, Business Requirement gathering, Concept building, Technology solution evaluation, Request for Proposal building, Business Case binding, consider required Compliance and Standards, Risk Assessment in all possible aspects to build confidence among signing authorities to reduce operational cost, operational risk, reduce rework, improved performance and ensure sustainability.

Educate all involved parties on policies, procedures and guidelines to the below agreed process / pipeline steps: Ensure top-down approach ad bottoms up enablement.

i. Define and agree a Concept Note (Organizational Unit needs an IT solution by a specific date by not exceeding the budget of X amount)

ii. Define, Agree and Distribute Request for Proposal(RFP)

iii. Evaluate Product / Solutions
iv. Define and Agree a Must & Want
v. Assess Strategical Risk
vi. Assess People Risk
vii. Assess Financial Risk
viii. Assess Architectural Risk
ix. Legal Risk
x. Define and Approve Business Case
xi. Run Project
xii. Audit Project Phases
xiii. Manage Changes
xiv. Asses Compliance
xv. Manage Incidents and Problems
xvi. Manage Issues and Risks
xvii. Handover to Operations
xviii. Run Post Project reviews

b. Define and agree on KPIs for each phases

What metrics and KPIs should organizations track to measure the effectiveness of their GRC approach in achieving information security goals? How do these metrics inform continuous improvement efforts?

All projects, new initiatives, request management, changes and incident fixe process must go through the collectively agreed GRC pipeline activities and phases, which operates with adequate controls, measures and reporting in line with Compliance and Risk Management mandates. Some examples of KPIs:

i. Number of concept notes raised by organizational units
ii. Number of concept note approved by the organizational management
iii. RFP responses in numbers
iv. Must and Wants scoring
v. Evaluations results and comparison
vi. Risk Assessment report
vii. Number of business cases reviewed with Risk Assessment
viii. Audit and Assess control on each phases of the project/ changes
ix. Mange issues / risk log
x. Manage changes and problems
xi. Post implementation reviews
xii. Performance monitoring and reporting
xiii. Project / Change closure audit report (COBIT based)
xiv. Benefit realization report
xv. Weekly Average operational incidents

AI TO SHAPE DUBAI'S NEXT 185 YEARS OF DEVELOPMENT

Dubai is well on track to becoming a preferred global AI hub thanks to the concerted efforts of the government in partnership with the private sector in rolling out a slew of initiatives towards integrating the deep technology into government work and the social fabric, making the city an indispensable partner of choice for AI developers, startups, and companies from around the world, HE Omar Sultan AlOlama, Minister of State for Artificial Intelligence, Digital Economy, and Remote Work Applications, said.

The Minister welcomed more than 2,500 distinguished UAE leaders and AI experts, policymakers, government officials and industry stakeholders to the iconic Museum of the Future and AREA 2071, which jointly hosted the largest such gathering in the world. Participants engaged in conversations on AI legislation and policy, and on the ethical use of AI, as well as on the best ways of convening AI communities and talent. They also shared insights on facilitating the implementation of AI applications as tangible solutions to local and global challenges.

Emphasizing the importance of continually adapting with this dynamic technology, he urged everyone to utilize the available tools effectively to stay competitive and avoid falling behind in the global AI race.

"AlOlama stated that the UAE's visionary leadership, under the directives of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai and the visions of His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai and Chairman of the Executive Council of Dubai, seeks to develop a leading, proactive, and future-oriented model for Dubai and lead the AI conversation through the establishment of this platform and his recent announcement of 22 Chief AI officers in government departments across Dubai. AlOlama noted that each officer had been appointed after careful assessment of their skills to advance Dubai's AI vision. Another initiative is the training of one million proficient engineers. This effort is not merely because these skills will remain relevant in ten years, but because individuals possessing them can elevate their nation's power today."

His Excellency highlighted the leadership's belief in the importance of talent in building the future has resulted in the UAE ranking third globally in attracting AI talent relative to its population size, after Luxembourg and Switzerland, and first regionally - up from the 11th place in 2021, according to a report by LinkedIn in collaboration with Stanford University. The UAE also ranked 15th globally for its AI skills, up from the 20th place last year.

"AI is not a future vision; it is our reality now. In Dubai, we operate differently. Our long-term vision for our physical infrastructure was first implemented in 1958, and it took essentially 185 years until 2023 for Dubai's infrastructure to be considered among the best in the world. Similarly, with AI, we are looking at implementing our AI vision for the next 185 years, starting today," HE AlOlama said, urging the private sector to start their journey from Dubai to invest in AI and enhance their talents for its enabling legislation, as much as because AI is integral to DUB-AI!

CYBER READINESS
BECOMES REALITY
WITH
COMMVAULT® CLOUD
CLEANROOM™ RECOVERY
Commvault®
Visit commvault.com to Learn More