CYBER DEFENSE MAGAZINE

eMAGAZINE

JUNE 2024

In This Edition

Special Cybersecurity Considerations for Medical and Legal Practices

Understanding the Dark Web: What You Need to Know

How and When to Know You Need a Fractional CISO

...and much more...

MORE INSIDE!

`

CONTENTS

@MILIEFSKY

From the

Publisher…

Rise Above the Noise!

We are pleased to announce that The Black Unicorn awards program is now part of the Top InfoSec Innovator awards program. Please see detailed information at the Conference and Awards website:

https://cyberdefenseconferences.com/top-infosec-innovator-awards-2024-apply-today/

We have a virtual red carpet already set up, with the incredible high traffic website and social media marketing, and much more to help bolster the good news around our winners during our 2nd half of 2024, 12th anniversary and 12th annual awards during CyberDefenseCon 2024.

World's First Cyber Defense Genius™

Also, please remember that Cyber Defense Magazine has launched the World's First Cyber Defense Genius™ the world's first AI GPT trained specifically on over 16,500 pages of infosec expertise and learning more, daily. It is now available on our home page at https://www.cyberdefensemagazine.com/ on the ride side of the screen. We welcome your comments and feedback as you take advantage of this excellent professional resource.

It Has Been 12 Amazing Years

When I founded Cyber Defense Magazine 12 years ago, there were only 300 cybersecurity companies worldwide, very few MSSPs and less than 100 million in worldwide damages on cybercrime. Fast-forward to 2024 and we are looking at many hundreds of billions in damages, potentially trillions in the coming years. We see the weaponization of artificial intelligence, data theft and the hundreds of billions of records, and 3500 cybersecurity companies and managed security service providers on the horizon with new and innovative ways to defend against the latest threats. The landscape continues to evolve but the fundamentals never change: managing your risk and increasing cyber resiliency are critical for any business to operate successfully in this heated cyber climate.

Our mission is constant - to share cutting-edge knowledge, real-world stories and awards on the best ideas, products, and services in the information security industry to help you on this journey.

Warmest regards,

Gary G. Miliefsky

Gary S. Miliefsky, fmDHS, CISSP®
CEO/Publisher/Radio/TV Host

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:
https://www.cyberdefensemagazine.com/about-our-founder/

12 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 WIRE WEBINARS
CYBERDEFENSECONFERENCES

Welcome to CDM's June 2024 Issue

From the Editor-in-Chief

With over 50 articles by expert authors from around the cyber security industry, we continue to experience a broadening of relevant topics responding to the practical needs of cyber professionals and non-technical users alike. Over the past year, coming across the Editor's desk, we have seen an increase in both the scope and number of articles addressing the growth of cyber-dependent activities.

This should not be surprising, since the rapidity of growth in cyber attacks and defenses could be considered a corollary or adjunct to Moore's Law. The number of exploits and defenses may not literally double every 2 years, but the breadth of organizational recognition of the importance of effective cyber security practices has certainly multiplied and spread throughout the community.

Once again, cyber risk and risk management, including prevention, insurance coverage, and recognition of new threats, are coming to the fore in our review of the submissions we receive from within the profession and beyond.

We would like to remind both readers and contributors that Cyber Defense Magazine is a nonpartisan publication. From time to time, we may publish an article reflecting a particular point of view with political implications. In those cases, we endeavor to include a disclaimer that such publication does not constitute an endorsement, but only reflects the perspective of the author.

As always, we strive to be the best and most actionable set of resources for the CISO community in publishing Cyber Defense Magazine and broadening the activities of Cyber Defense Media Group. With appreciation for the support of our contributors and readers, we continue to pursue our role as the premier provider of news, opinion, and forums in cybersecurity.

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

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

UNKNOWN CYBER

"70% of Malware Infections Go Undetected by Antivirus..."

Not by us. We detect the unknowns.

www.unknowncyber.com

2001 2024

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


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

We are Open XDR

Making Security Operations Simpler

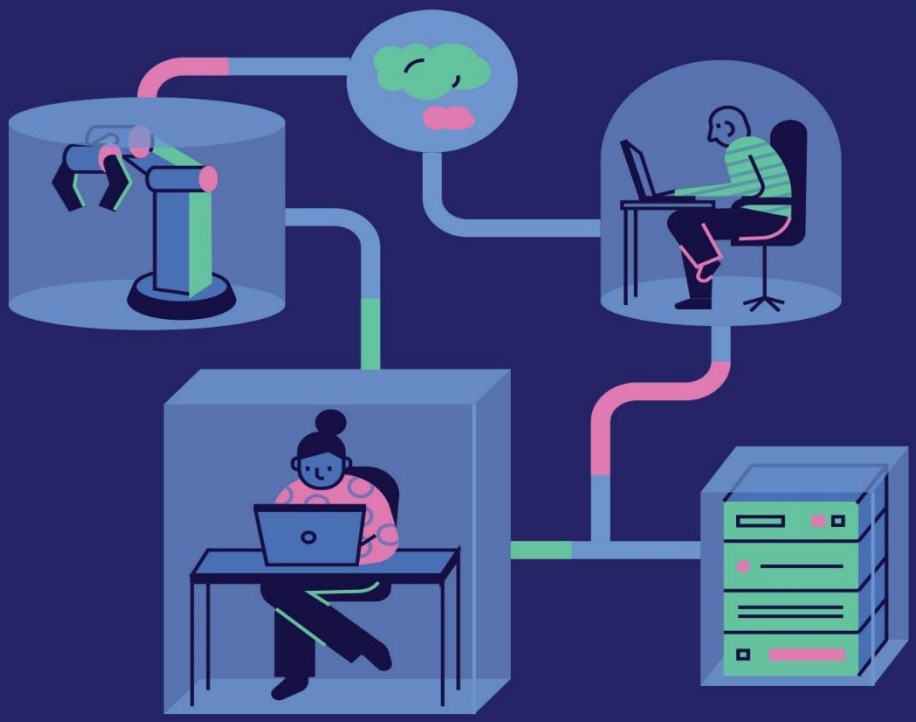
It's your security stack. Our job is to make it work better to deliver the security outcomes you need.

stellarcyber.ai

STELLAR CYBER®

ZERO.
Networks

Radically simple segmentation *in a click.*



Don't believe us?

Neither did they!

SCAN ME

zeronetworks.com

RIDGE SECURITY

RidgeBot® AI-Powered Security Validation Platform

Exposure Management

Automated Pentesting

Avoid Staff Shortage

RidgeBot® CTEM Support

Automates asset discovery, vulnerability assessment, and attack modeling, ensuring efficient exposure detection and resolution.

Learn More

Gartner Cool Vendor

SC 2023 awards EUROPE highly recommended

IDC Innovator

ImmuniWeb®
AI for Application Security

Gartner peer insights
4.9 out of 5

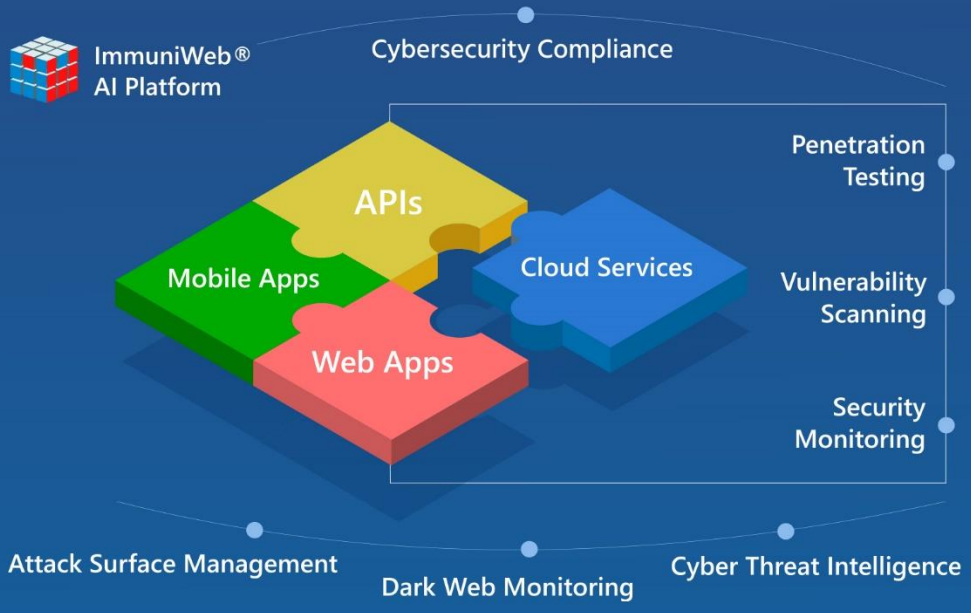
Risk-Based and Threat-Aware Application Security Testing (AST)

Traditional Application Security

- Vendor 1 — Penetration Testing
- Vendor 27 — Risk Management
- Vendor 9 — Security Scanning
- Vendor 11 — Attack Surface Management
- Vendor 22 — Cyber Threat Intelligence
- Vendor 17 — Dark Web Monitoring

vs

ImmuniWeb® AI Platform



ebay · next bank CRÉDIT AGRICOLE · ITU · BDO · SIX · haymarket · unifiscgroup · Swissquote

Award-Winning Technology. 20 Use Cases.

- Web Penetration Testing
- Third-Party Risk Management
- Cloud Security Posture Management
- Mobile Penetration Testing
- Attack Surface Management
- Red Teaming Exercise
- Dark Web Monitoring
- API Penetration Testing
- Web Security Scanning
- Cyber Threat Intelligence
- Continuous Penetration Testing
- API Security Scanning
- Continuous Automated Red Teaming
- Mobile Security Scanning
- Network Security Assessment
- Digital Brand Protection
- Phishing Websites Takedown
- Cloud Penetration Testing
- Software Composition Analysis
- Continuous Breach and Attack Simulation

CREST ACCREDITED · ISO 9001 SGS · ISO/IEC 27001 SGS · UKAS MANAGEMENT SYSTEMS 005

One Platform. All Needs. **www.immuniweb.com**

DIB CONTRACTORS:

Nation-state and ransomware actors are targeting your data.

We can help protect it.

Get started - nsa.gov/ccc

FREE CYBERSECURITY SERVICES ARE AVAILABLE TO THE DIB
NSA CYBERSECURITY COLLABORATION CENTER

CYDERES

We will focus on your cybersecurity, so you can focus on your business.

We have the right mix of people, processes, and technology to build your robust security program and respond successfully to any threat that comes your way.

Cyber **De**fense
& **Res**ponse.

It's what we do.

cyderes.com


ARTICLES

Special Cybersecurity Considerations for Medical and Legal Practices

"Protect The Most Vulnerable at Their Most Vulnerable Times"

By Jim Ford, Founder and CEO, PatientLock® and JurisLock™

In the spring of 2018, my (then) pregnant wife and I went in for a 28-week sonogram of our twins. Like most soon-to-be parents, we expected it to be a fun, exciting visit, and another opportunity to see our babies in the womb. Little did we know it would turn out to be one of the scariest days of our lives.

Shortly into the exam, the sonographer looked troubled and quickly called a physician into the room, where it was discovered that our daughter was in distress. Our daughter was no longer able to effectively push blood back out through the placenta, causing her heart rate to continually decelerate. As a result, the medical staff informed us that both of our kids needed to be delivered immediately and that only a few hospitals in the area had NICU's (neonatal intensive care units) capable of supporting them.

Spoiler alert: While both kids came into the world weighing less than two pounds a piece, following a three-month stint in the NICU at Overland Park Regional Medical Center (HCA), (and six years later), we have happy, rambunctious, and perfectly healthy kindergartners.

The relevance to this (cybersecurity) story stems from the fact that we chose, in large part, to forego using a well-known pediatric hospital in our city because of breach events that had occurred beginning in 2016 and continuing through January 2018, resulting in the theft of approximately 70,000 patient records.

Between our two kids, the NICU bills (covered by insurance) were nearly $3-million dollars. Patient identity and safety concerns aside, the decision we made as parents and consumers had a detrimental monetary impact to the pediatric hospital in the form of a significant, lost revenue opportunity. Amongst others, that event, or I should say decision, poured gasoline on the vision I had in founding PatientLock, and a few years later, JurisLock. That vision (turned Mission) was to make "enterprise grade" cybersecurity available and affordable to any size of business using channels servicing the Defense community.

Those in the healthcare and legal professions, specifically, are tasked with protecting and serving patients and clients in some of their most vulnerable times. Their goal as professionals is to provide help during some of the most stressful, life-threatening, or otherwise impactful times an individual may ever go through. On the medical side, this could be delivering premature babies, assisting a patient through a cancer diagnosis and treatment, or making the end-of-life process as comfortable and painless as possible. On the legal side, this might be working with a client who has suffered a catastrophic injury. It might be a divorce, a child custody case, working through criminal/civil litigation matters involving freedom or one's life savings, or helping a business make a strategic acquisition.

I would not imagine that during these interactions, cybersecurity is priority one (or two, or ten, or twenty). However, because these professionals often meet and work with extremely sensitive information during their work, this information must be properly safeguarded. Otherwise, there can be significant, negative results. Cyber criminals could gain access to a provider's network, compromising a surgery already in process. Information in a patient's electronic medical record could be deleted, or changed (think allergies, dosing information, or other significant information like a patient's blood type), or a physician office or hospital could be locked out of its computers such that patient care is disrupted (also leading to significant revenue loss). Worse yet, a double extortion tactic including data exfiltration and ransomware might be used simultaneously. This occurs when a bad actor steals records to then sell on the Dark Web, while also executing a ransomware attack and demanding payment.

Due to these factors, those practicing law and medicine have special and unique obligations to protect the information of those they serve. Just to name a few:

- Doctor-patient privilege/attorney-client privilege
- Ethical obligations/ABA Rule 1.6
- HIPAA
- Special laws protecting substance abuse information
- State law requirements

The practice of law and medicine have in common several important features, in particular the doctor-patient privilege and the attorney-client privilege. The goal of both of these is to ensure that proper care can be provided, without fear of repercussion (whether disclosure publicly or introduced as evidence in a lawsuit). If a patient or client cannot provide full details, their practitioners can't provide proper service. Often these details could be embarrassing, could lead an individual to believe the information could be used against them in a different context, or an individual may not understand that what they see as a trivial bit of information could be extremely important for their medical or legal professional.

This is where the tie-in to cybersecurity comes into play. Cyber criminals know that those in the medical and legal professions house some of the most sensitive data, and that such information, if made public, would have negative ramifications. Cyber criminals also know that, if hit with ransomware, these professionals are likely to pay the ransom to ensure this information is not made public and/or that these professionals can continue to provide uninterrupted service to a vulnerable audience.

PatientLock and JurisLock were developed specifically with the most vulnerable in mind. PatientLock and JurisLock have bundled services specifically designed to harden a healthcare organization or law firm's cybersecurity posture through a fully managed suite of cybersecurity technology and compliance/advisory services, designed to force-multiply IT resources and satisfy regulatory frameworks and rules like HIPAA, PCI, NIST, ABA Formal Opinions, as well as cyber insurance requirements.

PatientLock's and JurisLock's Security Operations Centers (SOCs) are the same that provide service to the DOD and the largest military-defense-contractors in the world, allowing clients to take advantage of previously unattainable economies-of-scale. With 400+ cybersecurity professionals, PatientLock and JurisLock eliminate the need to hire security staff and solve the talent issue by managing the security technologies (MDR, XDR, MEDR, VUMA, EPS, etc.), monitoring for threats 24/7/365, and taking action in real-time to address them.

In our experience, it's become clear that it's often the case that C-Suite executives just don't know what they don't know (NOT a typo). Among other duties, a CISO's responsibilities include educating decision-makers on cyber risks and risk management. Most small and medium-sized organizations don't need or can't afford to hire a full-time CISO. PatientLock's and JurisLock's virtual vCISO program provides a fractional CISO to exercise oversight of enterprise-wide cybersecurity and governance, while helping achieve compliance for regulatory frameworks including NIST CSF and HIPAA Compliance, Security Risk Assessments, HITRUST and SOC2 Readiness, GAP Assessments, and more.

We recognize that technology alone isn't enough. Cyber insurance can also protect organizations against many different risks associated with cyber incidents, especially since cyber incidents are often not adequately covered, or covered at all, by D&O or E&O policies. Cyber insurance is designed to help an organization mitigate exposure through risk transfer by offsetting costs associated with responding to an incident like data and system recovery, business interruption, extortion expenses and claims and lawsuits asserted by others directly affected by the incident. We see cyber insurance as a risk management device similar to commercial property coverage for a fire in a restaurant's kitchen. Even though restaurants have sprinkler systems, extinguishers, fire alarms, etc., a restaurant would never forego having property insurance because it mitigates the damage that the inevitable kitchen fire will cause.

In practice, PatientLock and JurisLock have found that “stapling” our documentation to a cyber liability insurance application provides underwriters and carriers the opportunity to increase the limits of risk transfer offered, lower annual premiums, reduce retentions, and offer broader coverage options for PatientLock and JurisLock customers.

We started with a simple goal: to protect the most vulnerable at their most vulnerable times. It started with the trip to the NICU several years ago, and the needs and risks have only continued to grow. Cyber criminals are making things as complicated as possible, and the potential impact of a breach is now more devastating than ever. However, we will continue to work with those in the medical and legal professions to protect those that they serve. There are steps that those in these fields can take to limit this risk, and we are here to help them on that journey.

About the Author

Jim Ford, Founder and Chief Executive Officer of PatientLock and JurisLock. Prior to founding PatientLock, Jim spent nearly two decades working in healthcare, or healthcare information technology, beginning his career in the laboratory of an HCA hospital in 1998. Prior companies include Cerner, athenahealth, Aprima/eMD’s, and Fortified Health Security, a healthcare focused managed security services provider, or MSSP.

Jim founded PatientLock in 2019 with the vision of making enterprise-level cybersecurity technologies and services available and affordable to any size of healthcare organization. PatientLock is now deployed on network assets used by thousands of US-based healthcare organizations.

Following the successful launch of PatientLock, Jim was approached by legal professionals looking to address the cybersecurity and compliance issues faced by law firms. JurisLock was then launched for law firms where the handling and storage of personally identifiable information (PII) and electronically protected health information (ePHI) create the same compliance requirements and cybersecurity challenges faced by healthcare organizations.

Jim earned certification as a HITRUST Practitioner, (CCSFP) was certified by the Supremus Group as a HIPAA Privacy and Security Expert - Level-4 (CHPSE) and holds a master’s degree in business administration (MBA).

Jim can be reached online at jford@patientlock.net and at the PatientLock or JurisLock company websites: https://patientlock.net/ or https://jurislock.com/

Understanding the Dark Web: What You Need to Know

Exploring the Dark Web: Essential Insights Revealed

By Elena Thomas, Digital Content Strategist, SafeAeon Inc.

The internet is like a huge iceberg: there is a hidden layer below the top. The dark web is the name for this hidden world that is often wrapped in mystery and false information. There are a lot of websites and groups that regular search engines can't reach in this area, which makes up about 5% of the whole internet. You can use the clear web every day, but to get to the dark web, you need special software like Tor to hide your behavior and let you into this secret online territory.

Interesting, right? But be careful before you fall down the rabbit hole. There are good and bad things about the dark web. On the plus side, it gives activists and people who blow the whistle in oppressive governments a safe place to talk to each other. It's like a secret printing press—a place where you can tell the truth to powerful people without worrying about getting in trouble. Journalists can also use the "dark web" to get the private information they need for their investigations.

There is, however, another side to this digital coin. The same obscurity that helps the good guys also makes it easier for bad people to do bad things. People sell drugs, guns, stolen data, and hacking tools on the dark web, which is known as a market for illegal goods and services. It's a spot where thieves operate "out of sight, out of mind," which makes it a constant problem for police.

So, is the dark web a bad guy or a hero who people don't understand? The answer is hard to pin down, just like the dark web. In this digital age, it's important to understand this mysterious part of the internet. Whether you're a curious netizen or someone worried about their safety, you need to know what you're doing and be careful. In what follows, we'll take a closer look at the dark web, showing you its possible benefits and the risks that are built in.

Understanding the Deep Web vs. the Dark Web

Millions of people go to private parts of the internet every day, like their email inboxes and online banking accounts. These are parts of the "deep web," which is made up of places that search engines don't crawl and that are guarded by passwords and other security measures. The deep web is where about 90% of all internet material is stored and is used by businesses, the government, and nonprofits.

The dark web is a smaller part of the deep web that can only be reached with special tools like the Tor browser. The dark web is legal to reach and use, but most people who use the internet don't need to go there.

Origins and Development of the Dark Web

Ian Clarke created Freenet at the University of Edinburgh in 2000. It was a place where people could talk and share files anonymously. This was the start of the idea of the "dark web." This new idea paved the way for the Tor Project, which started in 2002 and later launched its browser in 2008, which lets people browse the web without being tracked.

Functionality of the Dark Web

The dark web was created so that the U.S. Department of Defense could communicate securely. Now, it's used by people all over the world who want to remain anonymous. Onion routing is used, a method that encrypts user data by sending it through multiple nodes. This protects privacy and makes tracking very hard.

Legal Uses of the Dark Web

The dark web has a bad image, but there are good reasons to use it. It gives people a way to talk to each other freely in places where the government controls and watches what they say. It's often used by activists, writers, and people who blow the whistle on wrongdoing to safely share information. Users

should be careful, though, and keep their security up to date with things like VPNs, private email addresses, and software that is always up to date.

Things That Are Illegal on the Dark Web

Because the dark web is anonymous, it also draws people who do bad things. People who sell illegal things like drugs, weapons, and stolen data do very well in this secret part of the internet. Famous websites like Silk Road, AlphaBay, and Hansa have been shut down by the government after it was found that they were running illegal businesses. Because people can remain anonymous on the dark web, hackers and law enforcement continue to face problems.

It's important to know about these parts of the deep and dark web to understand how they affect internet privacy, safety, and legal activities.

Key Insights About the Dark Web:

Targeted Searching

It's not easy to get around on the dark web. You can't use search tools to find your way around like you can on the surface web. Vice President at Peraton John M. said, "The dark web requires patience and a certain set of skills to search for information by hand and make sure it is correct." Websites and platforms often disappear or change, so users have to take extra steps to find the information they need.

High Risk of Malware

There aren't many rules about the dark web, which makes it more likely that you'll find malware. "Many sites that can be reached through the Tor browser have malware on them," warns John M. To lower your risk, he says to use a disposable machine that can be cleaned up after your exercise. Also, accidentally viewing illegal content can get you in trouble with the law, which is another reason to be careful when you're browsing.

Used by Organizations to Improve Security Tools like Peraton's Tornado are used to search the dark web by groups like the government. Every 30 days, this tool searches the dark web secretly for mentions of the group using specific keywords to find possible threats. This proactive method helps get ready for cyber threats and lessen their damage before they get worse.

A Refuge for Privacy and Whistleblowing

You can be more private on the dark web than on the open web. It's an important tool for people who want to blow the whistle on government corruption and get around censorship. For example, in the early days of the COVID-19 pandemic, Chinese people shared information without being blocked on the "dark web," which made it much less likely that the government would punish them.

Interactive Forums Dominate

Instead of static web pages, a lot of the dark web is made up of secret forums that are often encrypted. Most of the time, you need to be invited to join these groups to have private conversations. Being a part of these forums is important for gathering information because they often have unfiltered, real-time conversations. Federal organizations sometimes keep an eye on these forums to look into crimes and gather information about them.

Conclusion

The Dark Web is a complicated part of the internet that many people get wrong. It gives you protection and anonymity, which can be used for both legal and illegal reasons. It is a haven for people who want to protect their privacy, journalists, and people who are living under harsh governments. However, it is also known for being a place where illegal activities like trafficking, selling drugs, and cybercrime happen. Cybersecurity workers need to know about the "Dark Web" to fight cyber threats and keep company assets safe. People should be careful when they use the Dark Web because it could be dangerous and their online actions could be illegal. As long as users stay informed and aware, they can better manage the Dark Web and protect themselves from its darker sides. It is important to find a balance between using its benefits for good and being aware of the risks it brings.

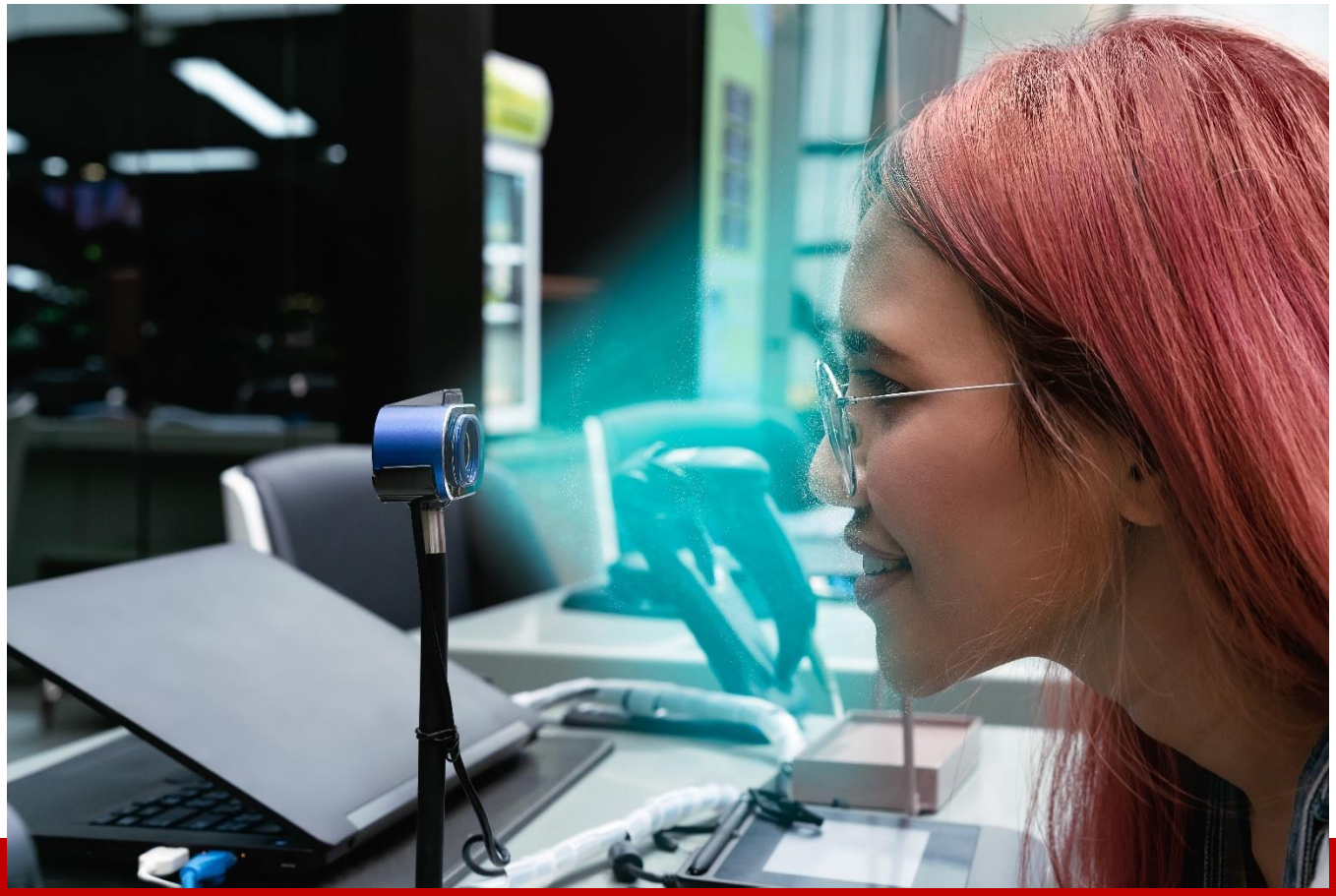
.

About the Author

Elena Thomas is the Digital Marketing Manager at SafeAeon, a leading cybersecurity company, where she combines her passion for digital marketing with her unwavering dedication to enhancing online security. With a career spanning over a decade in the cybersecurity realm, Elena has emerged as a prominent figure in the industry. Her expertise lies in crafting innovative digital strategies that empower individuals and organizations to safeguard their digital assets.

Beyond her professional life, Elena is a true cybersecurity enthusiast. She devotes her spare time to educating the public about the ever-evolving cyber threats and how to stay protected in the digital age. Elena's commitment to a safer digital world shines through in her informative and engaging writing, making her a sought-after contributor to blogs and publications in the cybersecurity space. When she's not immersed in the world of cybersecurity, Elena enjoys outdoor adventures and exploring new cuisines.

Elena can be reached via email at elena.thomas@safeaeon.com and at our company website http://www.safeaeon.com/ .



How and When to Know You Need a Fractional CISO

By Andy Hilliard, CEO of Accelerance

Every business owner knows how important cyber security is. Headlines of attacks, leaks and breaches of customer data, payment information, intellectual property and more emphasize that need almost daily. But not every business can afford to pay a chief information security officer on a full-time basis. Enter the fractional CISO.

Fractional CISOs are ideal for businesses that want to stay safe and secure while watching their budgets. A fractional CISO will help ensure that your platforms are up to date, that any onsite and offshore teams are operating securely and that systems run smoothly. That includes full-time IT staff and project developers.

But how can you tell that you need that expertise? When should you bring in a fractional CISO? Experiencing a data breach or other cybersecurity attack is an obvious sign you need to up your

cybersecurity gameplan. But don't wait for trouble to strike. The right fractional CISO at the right time can help you prevent or prepare for attacks.

What are some of the indicators you should watch for?

- **Rapid Growth Without Corresponding Security Maturity:** If your organization is experiencing rapid growth in terms of revenue, market share, or workforce, but your cybersecurity measures are not maturing at the same pace, a fractional CISO could provide the necessary strategic direction.
- **Complex Regulatory Compliance Needs:** For businesses in heavily regulated industries (like finance, healthcare, or energy), staying compliant with evolving regulations requires sophisticated security strategies. A fractional CISO can help you navigate these complexities effectively.
- **Increased Frequency of Security Incidents:** A rise in minor security incidents or "near misses" can be a precursor to more significant breaches. A fractional CISO can help identify root causes and improve your security posture over time.
- **Lack of Cybersecurity Leadership:** In the absence of a clear cybersecurity strategy and leadership, organizations may struggle to prioritize and implement effective security measures. A fractional CISO can often bring confident leadership as well as a strategic viewpoint to your organization.
- **Business Model Evolution or Digital Transformation:** As organizations undergo digital transformation or pivot their business models, new security vulnerabilities can emerge. A fractional CISO can guide your secure adoption of new technologies and processes.
- **Supplier and Partner Security Requirements:** Increasingly, businesses are required to demonstrate robust cybersecurity measures to engage in partnerships or serve clients, especially in B2B environments. A fractional CISO can ensure that your security practices meet or exceed these expectations so your business gets what it needs.
- **Difficulty Attracting or Retaining Cybersecurity Talent:** The cybersecurity field is highly competitive, with a significant talent shortage. A fractional CISO can fill the leadership gap and help build a stronger internal team by defining roles, responsibilities, and career paths clearly.
- **Unclear Security ROI:** If your organization struggles to understand the return on investment for security initiatives, a fractional CISO can help align security spending with business objectives and demonstrate value.
- **Board-Level Concerns About Cyber Risks:** When board members express concerns about cyber risks and the organization's readiness to address them, it's a clear signal that the expertise of a fractional CISO could benefit both strategic planning and board communications.

More subtle, less obvious, indications your organization could benefit from a fractional CISO often include:

- **Inconsistent Security Policies Across Departments:** When security policies vary significantly between departments, it can indicate a lack of cohesive cybersecurity strategy, potentially leading to vulnerabilities.

- **Over-reliance on Legacy Systems**: An organization's reluctance to upgrade or patch legacy systems due to operational dependency, fearing disruptions, can create security risks. This reluctance might not be openly discussed but is a critical vulnerability.
- **Unregulated Shadow IT**: The use of unsanctioned software or hardware by employees without IT approval (known as Shadow IT) can expose the organization to risks. You've got Shadow IT in place when departments start solving IT problems on their own, bypassing official channels.
- **Frequent Exception Requests to IT Policies:** Regular requests from employees for exceptions to IT policies may indicate that the policies are outdated or not aligned with business needs, potentially leading to security gaps.
- **High Employee Turnover in IT Security Roles**: While not often linked directly to cybersecurity risks, high turnover can indicate underlying issues with the organization's security culture or a lack of clear strategic direction.
- **Lack of Security Awareness Among Employees**: Subtle indicators, like casual discussions that reveal ignorance about phishing or the importance of strong passwords, can suggest that the organization's security training is insufficient.
- **Vendor Management is Overlooked:** If discussions with suppliers and partners rarely include security considerations, it may indicate an underestimation of supply chain risks.
- **Limited Engagement with Industry Security Groups and Standards:** Not participating in or following industry cybersecurity groups or standards might indicate an organization's lack of proactive engagement with the cybersecurity community.
- **Silence Around Cybersecurity:** In some organizations, the absence of regular communication about cybersecurity, whether in meetings, reports, or newsletters, can itself be a warning sign. It may suggest an underestimation of cybersecurity importance at the executive level.
- **Resistance to Security Audits or Assessments**: A subtle reluctance or defensiveness when external security audits or assessments are proposed can signal an organization's fear of uncovering and confronting its cybersecurity vulnerabilities.
- **Disproportionate Focus on External Threats Over Insider Threats:** Exclusively focusing on protecting against external attackers without considering the risk of insider threats can be a critical oversight.

Each of these points to underlying challenges in managing cybersecurity effectively at a strategic level.

A fractional CISO can also help your organization move from being reactive to proactive. It's hard enough stomping out day-to-day IT fires, not to mention juggling those same resources for longer term projects. You need a holistic approach that addresses the root causes of security issues.

They can guide this transition with specialized skills and activities such as conducting deep-dive risk assessments, building a security strategic plan and roadmap and more. By emphasizing the identification and resolution of root causes, a fractional CISO enhances the organization's immediate security posture and builds a foundation for long-term resilience against cyber threats. This strategic approach ensures that cybersecurity efforts are efficient, effective, and aligned with the organization's broader goals and risk tolerance while creating long-term value.

A fractional CISO brings expertise, leadership, and an external perspective that can help organizations navigate these challenges and more, enhance their security posture, and align cybersecurity strategies with business objectives.

About the Author

Andy Hilliard is the CEO of Accelerance. He leads the globalization and collaboration of software teams with companies seeking talent, innovation, and a globally-distributed extension of their engineering function. Hilliard recently released his latest book, Synergea: A Blueprint for Building Effective, Globally Distributed Teams in the New Era of Software Development. Andy can be reached online at www.linkedin.com/in/andyhilliard/and at www.accelerance.com/.

Insights from RSA Conference 2024: Transformative Innovations in Cybersecurity

Beyond the Buzz Word AI, the Practical Groundbreaking Stuff

By Samridhi Agarwal, Masters Student, CMU

My first RSA Conference! Oh, what a blast it was! Attending the RSA Conference has been a long-held dream since I started in the cybersecurity field. The journey to make this dream come true began in January when I saw the incredible list of keynotes and speakers for RSA 2024. It surpassed my wildest dreams when I was selected for the Young Women in Cyber award, giving me the amazing opportunity to attend RSA 2024 with a press pass. Yes, a press pass! This was the cherry on top, allowing me to interact with and interview CISOs, CTOs, CEOs, and others from organizations doing groundbreaking work in cybersecurity.

To prepare for the conference, I read about various technologies and scheduled my calendar to make the most of the experience. However, once I arrived, I realized no amount of preparation could match the event's scale. It was massive, with organizations hosting their own launches, the Expo featuring impressive demonstrations, and countless amazing people to talk with.

While everything at the conference was fascinating, I particularly enjoyed the work of a few organizations in the cyber arena and loved learning more about the groundbreaking efforts their teams are making in the field. From developing advanced security technologies to pioneering new methods for protecting digital infrastructure, these organizations are at the forefront of making our digital lives more secure. In this trip report, I am covering some of these amazing people I talked with and the organizations they represent.

HORIZON3.ai: Revolutionizing Penetration Testing with NodeZero

In discussion with Snehal Antani, Co-Founder and CEO of HORIZON3.ai, we explored how organizations are constantly under threat from sophisticated attacks such as APTs, ransomware, and other malicious actors. Traditional penetration testing methods, while effective, are often labor-intensive, expensive, and time-consuming, making it challenging for businesses to keep up. HORIZON3.ai is addressing this critical issue with their groundbreaking solution: **NodeZero, an automated penetration testing platform** that combines human expertise with machine automation.

Node Zero automates many of the time-consuming aspects of penetration testing, allowing human experts to focus on more complex tasks and analysis. It provides detailed reports with remediation information, making it easier for organizations to address vulnerabilities and comply with industry standards. It clearly explains the sequence of events leading to critical impacts, providing proof of exploitation and detailed descriptions of necessary fixes. One feature of the dashboard that I particularly liked is its design, catering to users of all skill levels, from early career IT professionals to seasoned pen-testers; NodeZero makes penetration testing accessible and efficient.

Snehal Antani said "We are not making just another AI solution. It's an autonomous system that embodies a human-machine teaming approach," He explained, that this approach leverages the strengths of both human penetration testers and automated tools, providing a more comprehensive and scalable solution. The platform offers transparency and visibility into ongoing operations, allowing clients to monitor running modules, discovered issues, and network connections in real time.

HORIZON3.ai's NodeZero platform (Figure 1) is revolutionizing the way organizations approach cybersecurity. By providing continuous, autonomous penetration testing, it helps organizations proactively identify and fix vulnerabilities, ensuring a robust defense against sophisticated cyber threats. With its innovative features and user-friendly design, setting new benchmarks in the cybersecurity industry, empowering organizations to secure their digital assets effectively.

Clients have praised Horizon3.ai for the transformative impact of NodeZero on their cybersecurity strategies. A Senior IT Security and Risk Specialist shared, "NodeZero has given our organization the ability to conduct penetration testing in a reliable, repeatable, and affordable manner. The insights we gain from the platform are invaluable in strengthening our security posture."

Overall, the aim is to revolutionize the internal penetration testing process by providing a more efficient, accurate, and secure solution that combines human expertise with machine automation, while minimizing the attack surface and providing detailed, actionable reports for remediation to the clients.

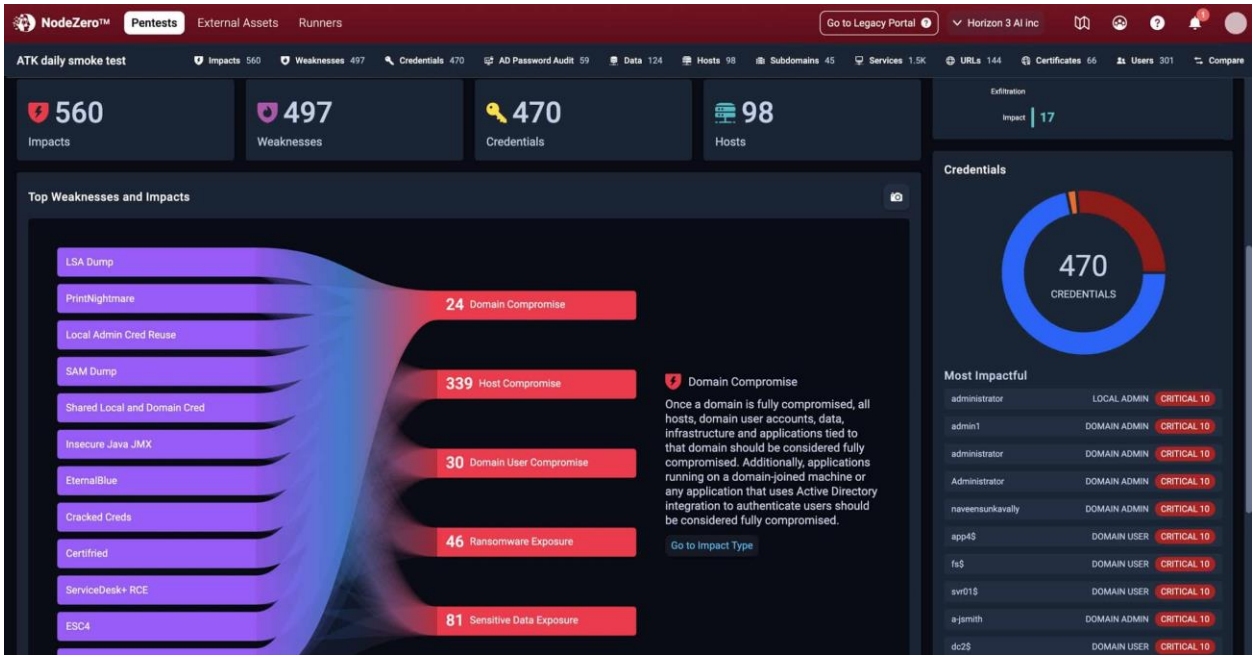


Figure 1: NodeZero Platform

RAD Security: Revolutionizing Cloud Security with Proactive Approach

In a conversation with Brooke Motta, the CEO and Co-Founder of RAD Security, we delved into how RAD Security is transforming cloud breach detection and response. As a behavioral cloud-native detection and response company, RAD Security provides the ultimate source of truth for cloud breaches by **behavioral fingerprinting** i.e. proactively fingerprinting unique environments, enabling the detection of novel attacks in real-time.

Traditional approaches to cloud security often rely on identifying millions of potential attack signatures, which is both time-consuming and inefficient. RAD Security takes a different approach by observing known good behavior and flagging any deviations as suspicious. For instance, fingerprinting sshd with RAD would have detected the XZ Backdoor attack immediately.

RAD Security provides a comprehensive three-in-one solution (Figure 2), focusing on the critical areas targeted by attackers today: cloud native infrastructure, identity, and the software supply chain. This holistic approach enables organizations to embed runtime fingerprints into their supply chain pipelines, detect novel attacks during runtime, identify malicious insiders, and strengthen their shift-left security programs. As Brooke Motta emphasized, securing cloud native environments has become the most critical task for CISOs, as these environments underpin the massive developments in artificial intelligence (AI). To secure AI, it is imperative to secure the underlying cloud native environments, including containers and Kubernetes. The statistics are compelling: 70% of teams are currently using containers

in production, and analysts predict that by 2025, 95% of new applications will be built using cloud native workloads. [1]

Clients of RAD Security have praised the platform for its transformative impact on their cloud security strategies. Raj Umadas, Director of Security at ActBlue, shared, “As long as I have RAD Security deployed and not throwing concerning alarms, I know our baseline is good.”

I was personally fascinated when Brooke Motta also highlighted the importance of diversity and inclusion in cybersecurity, encouraging a culture that supports women in the field. RAD Security sets itself apart by providing a proactive approach to cloud security, enabling organizations to detect and respond to attacks as they happen, rather than relying on reactive, signature-based detection methods.

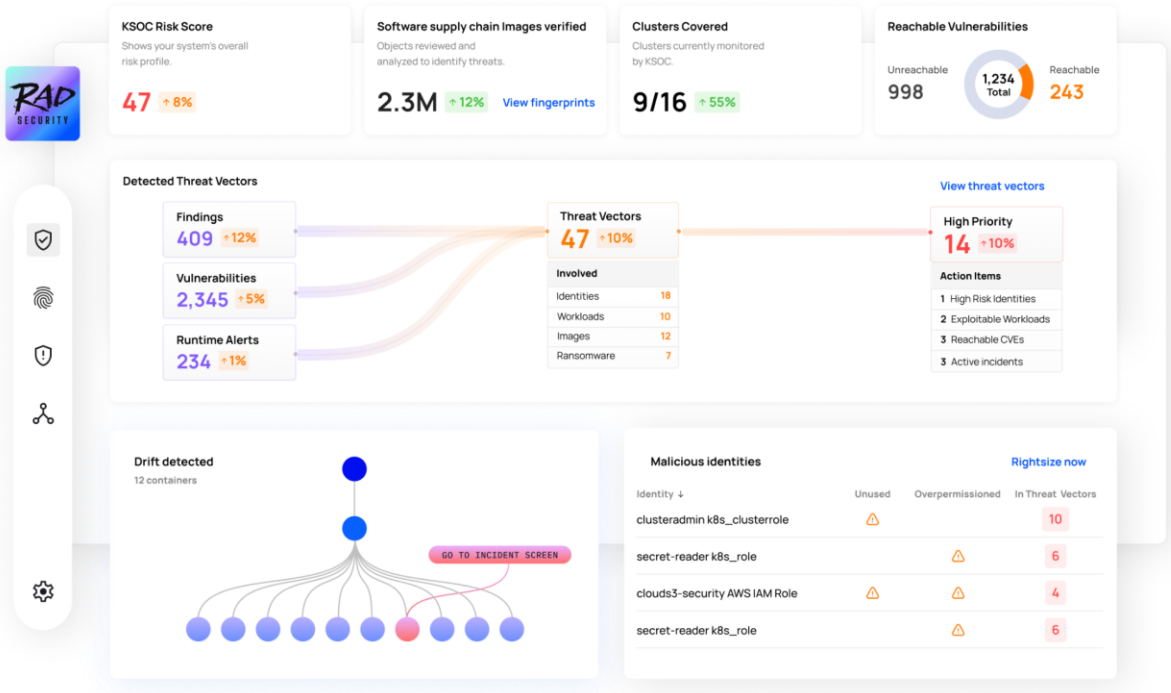


Figure 2: RAD Security Dashboard

Zentera Systems: Pioneering Zero Trust Security for the Modern Enterprise

In today's digital landscape, where traditional network perimeters have become increasingly porous, enterprises face a daunting challenge: securing their critical assets and data against sophisticated cyber threats. Hackers can breach the corporate perimeter through various means, and once inside, they have ample time to study the organization and craft custom attacks that are difficult to defend against. The consequences of a successful cyberattack can be devastating, with costs often exceeding $100 million to remediate an attack that occurs over a single weekend.

Zentera Systems offers a game-changing solution to this problem: the **CoIP Zero Trust Fabric**. As discussed with President and CEO Jaushin Lee, this solution implements the NIST SP800-207 specification for a Zero Trust Architecture, effectively defending assets and data against ransomware, lateral attacks, insider threats, and data leaks.

The CoIP Zero Trust Fabric deploys a new layer of airtight protections around critical assets and data, ensuring that every single network access is known and authorized. This proactive approach neutralizes threats to critical assets with effective cybersecurity protection, addressing the limitations of traditional network firewalls, threat detection tools, and monitoring. What sets Zentera apart is its unmatched speed, unparalleled simplicity, and incredible agility in deploying Zero Trust security. As Jaushin Lee emphasizes, “Our CoIP Platform provides award-winning Zero Trust networking, security, and multi-cloud connectivity that overlays on top of any infrastructure in any fragmented environment, allowing customers to be up and running in less than a day.”

Zentera Systems has become a leader in secure and agile connectivity solutions for the digitally transformed enterprise.

DNSFilter: Revolutionizing DNS Security for the Modern Workplace

In today's digital landscape, where remote work and bring-your-own-device (BYOD) practices are increasingly prevalent, organizations face a significant challenge in securing their workforce from cyber threats. Traditional security solutions often fall short in providing comprehensive protection for a decentralized and mobile workforce, leaving organizations vulnerable to phishing, malware, and other cyber attacks. As discussed with Ken Carnesi, Chief Executive Officer and Co-Founder of DNSFilter, the company offers a revolutionary solution to this problem: **Protective DNS**. DNSFilter's approach is to secure organizations at the DNS level, effectively blocking threats before they can even reach the network or endpoints.

DNSFilter's Protective DNS solution serves as a first line of defense against cyber threats, filtering out malicious domains and preventing users from accessing compromised websites or resources. By leveraging advanced machine learning and external threat feeds, DNSFilter ensures comprehensive and up-to-date threat protection. The company boasts over 35,000 customers and 35 million monthly users, highlighting its widespread adoption and trust among businesses of all sizes. [2]

What sets DNSFilter apart is its unique combination of ease of use, comprehensive threat protection, and unwavering customer support. As Ken Carnesi emphasizes, “From the beginning, we've made sure our threat categorization is driven by machine learning and supplemented by external feeds—giving our customers the most complete product.” The DNSFilter dashboard (Figure 3), is designed to cater to users of all skill levels, providing clear and actionable insights into network activity. It offers detailed reporting on threats detected and blocked, allowing security teams to understand and respond to incidents promptly.

DNSFilter is revolutionizing DNS security with its innovative approach to threat detection and prevention. By combining speed, simplicity, and proactive measures, DNSFilter ensures that organizations are well-protected against the ever-changing landscape of cyber threats.

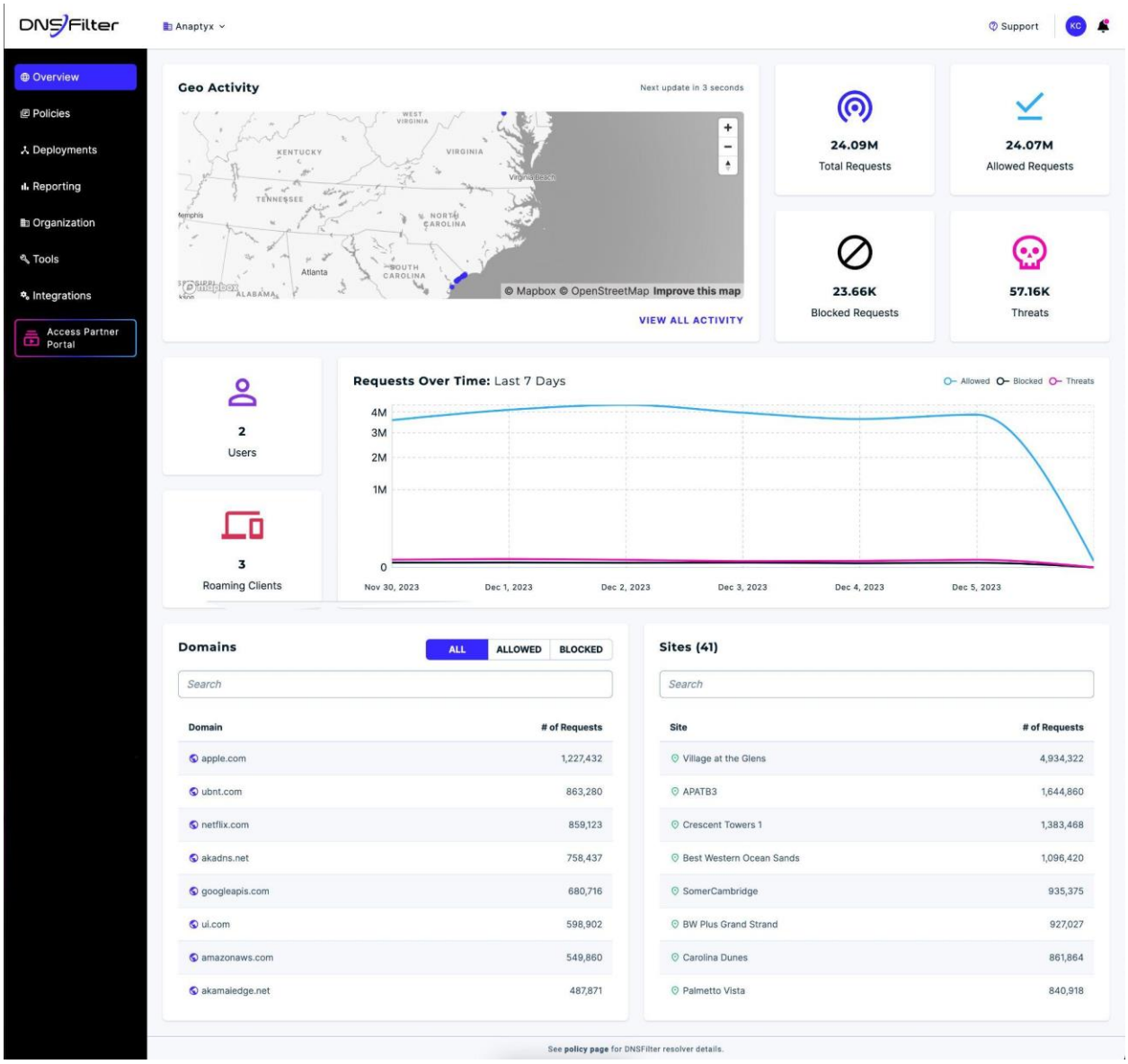


Figure 3: DNSFilter Dashboard

iboss: Revolutionizing Secure Access with Zero Trust SD-WAN

During my conversation with Paul Martini, CEO of iboss, I gained deeper insights into the cutting-edge solutions iboss is providing to address the complex security challenges of today's distributed digital environments. In the modern digital age, traditional security methods are proving insufficient to protect a dispersed workforce. Legacy SD-WAN solutions often necessitate the management of multiple disparate security technologies, complex routing, and cumbersome VPNs, leading to increased operational costs and inefficiencies. iboss tackles these challenges head-on with their **Zero Trust SD-WAN** solution. This innovation unifies iboss's industry-leading Zero Trust Security Service Edge (SSE) platform with Zero Trust SD-WAN, offering a comprehensive, single-vendor SASE (Secure Access Service Edge) solution.

This integrated platform (Figure 4) enables organizations to gain secure connectivity across their distributed environments while eliminating the need for legacy firewalls and cumbersome VPNs. By consolidating security and connectivity functions into a single platform, iboss simplifies IT management, boosts employee productivity, and significantly reduces organizational costs. As Paul Martini emphasizes, "At iboss, we are committed to continually advancing our technology to address the evolving needs of today's dynamic enterprise environments. With the launch of our Zero Trust SD-WAN, we are proud to offer a solution that not only meets the stringent security requirements of our customers but also enhances their overall productivity and reduces operational costs."

iboss's Zero Trust SD-WAN is a game-changer, providing a unified, efficient, and secure solution for today's distributed digital environments.

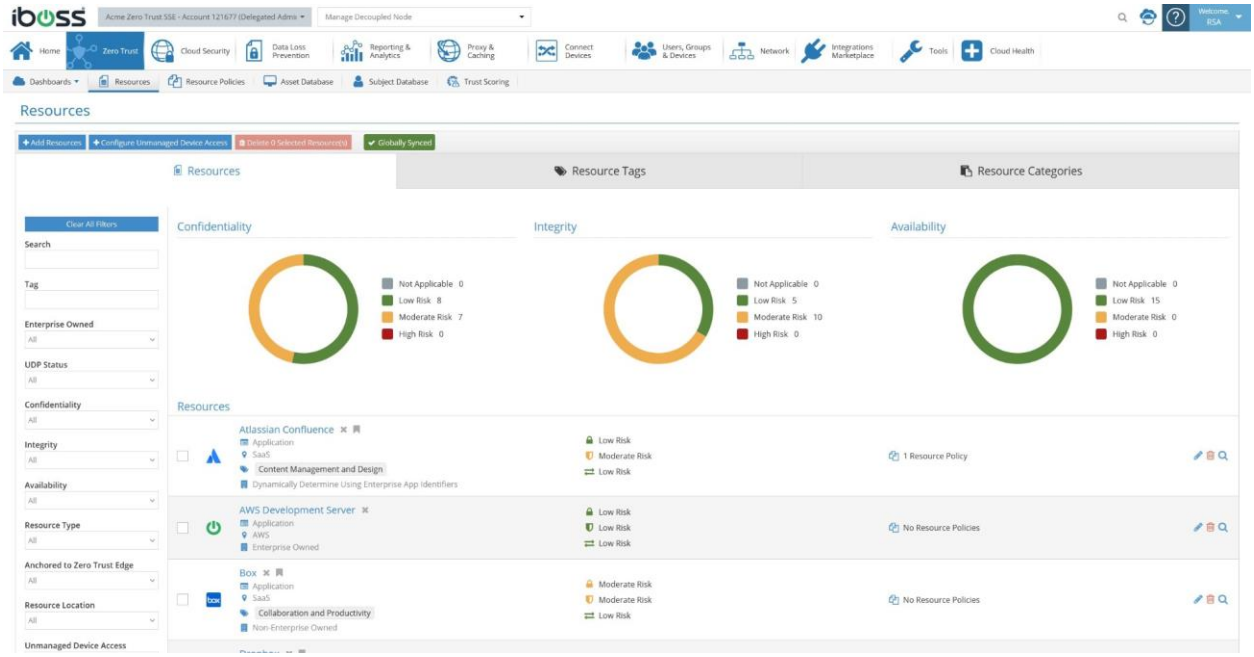


Figure 4: iboss Dashboard

A Remarkable Experience at RSA Conference 2024

To sum it all up, RSA Conference 2024 was amazing! I can't thank Cyber Defense Magazine enough for this incredible opportunity. It truly felt like a festival where everyone was united by a common goal – securing our digital space and pushing the boundaries of technology. I was amazed to see the collective efforts of so many brilliant minds coming together to make the RSA week an absolute hit. From groundbreaking product launches to insightful sessions and engaging networking events, the entire experience was simply mind-blowing. It was inspiring to witness firsthand the passion, creativity, and unwavering determination of industry leaders and innovators who are tirelessly working to fortify our digital defenses. I left the conference with a renewed sense of excitement and optimism for the boundless possibilities that lie ahead in the ever-evolving cybersecurity space.

References -

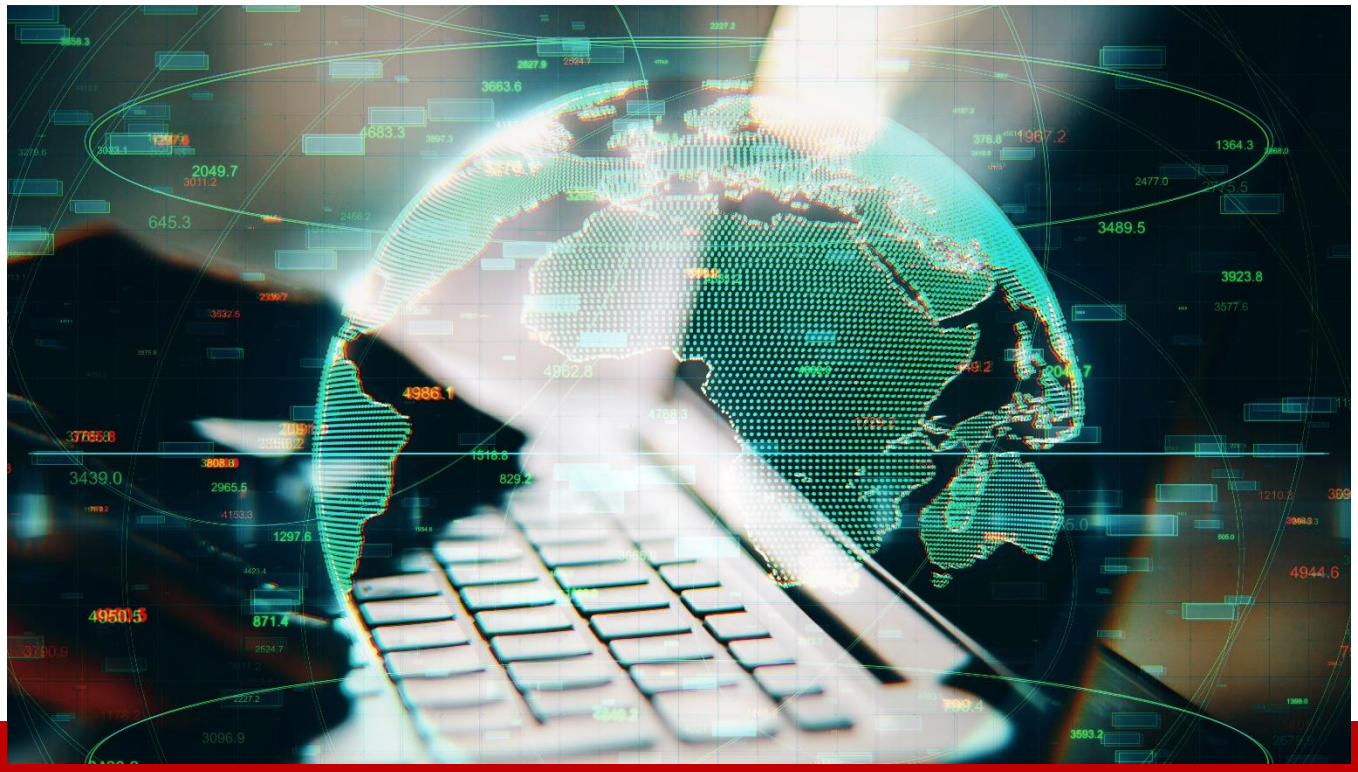
[1] Security, R. (n.d.). Cloud Security monitoring, management, and compliance basics. RAD Security. https://rad.security/blog/cloud-security-monitoring-management-and-compliance-basics

[2] Raymond, S. (2021, November 24). DNSFilter: DNS filtering: How does it work and why do you need it? DNS Filtering: How Does It Work? https://www.dnsfilter.com/blog/dns-filtering-how-it-works#:~:text=The%20short%20answer%20%3A%20DNS%20filtering%20gives%20you,with%20policies%20you%27ve%20determined%20you%20want%20to%20block.

About the Author

Samridhi is an award-winning woman in cybersecurity, reporter for Cyber Defense Magazine and currently pursuing a Master's degree in Information Security at Carnegie Mellon University. She is passionate about emerging technology and cybersecurity, with four years of industry experience as a cybersecurity associate and solution advisor. Throughout her career, she has collaborated with various clients and industries, analyzing their security infrastructure and implementing measures to address vulnerabilities in alignment with industry standards such as NIST and ISO27001. She is committed to continuous learning and exploring advancements to enhance global security and safeguard data.

Samridhi can be reached online at sam@cyberdefensemagazine.com



A National Imperative - Cyber Resiliency

Strategies to Safeguard Critical Infrastructure Against Cyber Threats

By Andrea E. Davis, Founder and President of The Resiliency Initiative

I started my career in emergency management in 1999. At the time, the focus was on the collapse of the world as we know it due to Y2K and computers not understanding the number 2. It seems rather silly after all the impactful crises we have dealt with since then. However, the concern and focus on our reliance on technology were justified. Fast forward 25 years, we are significantly more dependent on technology. Our technological systems, which are the backbone of our critical infrastructure, are increasingly vulnerable to cyber-attacks.

It feels like every day we wake up to the news of another cyber-attack, from pharmaceutical companies to healthcare operations to multinational computer companies. The FBI estimates that US consumers and businesses lost $12.5 billion to cybercrimes in 2023. The threats and the losses only keep increasing.

Earlier this year, FBI Director Christopher Wray testified before a House Select Committee on the vulnerability of US critical infrastructure. Director Wray stated that there is a threat of attack, especially from foreign actors, to sectors such as energy, water, transportation, communication, finance, and healthcare. Critical infrastructure systems are increasingly digitized and connected to the internet, making them vulnerable to ransomware, malware, phishing attacks, denial-of-service (DoS) attacks, and other cyber disruptions.

Our nation's critical infrastructure must be resilient to withstand and recover from these cyber disruptions. So, what are we doing about it?

Presidential Policy Directive 21 (PPD-21) advanced national policy to focus on the resiliency of the US critical infrastructure sectors. The Directive outlined the 16 essential infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so critical to the US that disruption would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof. Additionally, the recent publication of the National Security Memorandum on Critical Infrastructure Security and Resilience addressed our national vulnerabilities and created strategies to confront insidious cyber threats that have taken center stage from a national security standpoint.

These cybersecurity measures are essential to safeguard these infrastructure sectors from exploitation and disruption. Additionally, many critical infrastructure sectors are interconnected and interdependent. A disruption in one industry can have cascading effects on others. For example, a cyberattack on a power grid could impact transportation systems, communication networks, and healthcare facilities.

Let's examine a few incidents impacting the US infrastructure:

- For two days in August 2003, the US and Canada suffered one of the worst power outages in history, with over 50 million customers without power. It was concluded that the main cause of the outage was a “software bug,” not cyber terrorism. However, the US Department of Energy and Canada’s Ministry of Natural Resources created a task force to conduct a deep dive into the outage and provide recommendations on how to ensure similar outages don’t occur again. The final report stated that “procedural vulnerabilities were compounded by inadequate, out-of-date maintenance contracts.” Over 20 years later, the vulnerabilities that the report detailed still exist across the US electrical grid, and cyber criminals' sophistication has significantly increased.
- In May 2021, the US suffered one of its most significant critical infrastructure cyber-attacks - the Colonial Pipeline ransomware attack. The attack shut down Colonial Pipeline for five days, 45% of pipeline operators were impacted, panic buying ensued across the southeastern US, and significant supply chain disruptions were felt to an already strained system due to the COVID-19 crisis. The Colonial Pipeline attack highlighted the lack of government regulation when it came to reporting a cyber-attack on critical infrastructure and the lack of transparency to the US consumer once an attack occurred. The Colonial Pipeline attack led to the passage of the Strengthening American Cybersecurity Act (SACA), which created a reporting protocol and increased the Department for Cybersecurity & Infrastructure Security Agency’s (CISA) threat monitoring responsibilities.
- Finally, in early February 2024, over 70,000 AT&T customers were left without cell service, and multiple 911 call centers were out of service for close to eight hours due to a “technical error.” Over 70% of the US population relies on a cell phone as their primary mode of communication. Imagine a threat actor recreating a similar “technical error” throughout all cell phone networks in the US for several days.

Safeguarding our critical infrastructure requires a comprehensive and proactive approach involving collaboration, innovation, and continuous improvement in preparedness and response capabilities for the US to stay a step ahead of the cybersecurity threat.

I recommend the following four-pronged approach:

- **Developing Public-Private Partnerships:** Collaboration between government agencies, private sector organizations, and other stakeholders is crucial for protecting critical infrastructure. Public-private partnerships can facilitate information sharing, resource allocation, and coordinated responses to emergencies and cyber threats. The Federal Emergency Management Agency's (FEMA) Public-Private Partnership guidebook provides a solid framework and approach to establishing partnerships.
- **Investing in Comprehensive Emergency Preparedness and Response Plans:** Emergency management plans and protocols should address the unique challenges posed by cyber-attack disruptions to critical infrastructure. This includes conducting risk assessments, developing contingency plans, training personnel, and conducting exercises to test preparedness and response capabilities.
- **Increased Information Sharing and Coordination:** Timely and accurate information sharing among stakeholders is essential for effective emergency management and cybersecurity. Coordination between government agencies, law enforcement, industry partners, and international organizations helps to identify threats, mitigate risks, and respond to incidents efficiently.
- **Continued Investment in Technology and Innovation:** Continued investment in technology and innovation is necessary to enhance the resilience and security of critical infrastructure. This includes deploying advanced monitoring and detection systems, implementing secure communication protocols, and leveraging emerging technologies such as artificial intelligence and blockchain for cybersecurity.

About the Author

Andrea Davis is a world-renowned expert in the field of emergency management. Currently, Ms. Davis is the President and CEO of a Women Owned Small Business (WOSB), The Resiliency Initiative (TRI). Ms. Davis founded TRI out of a passion to serve the whole community before, during, and after an emergency. Ms. Davis has held leadership roles with NGOs (The American Red Cross, Save the Children US), the US Federal Government (FEMA, The Federal Reserve) and Fortune 500 Companies (Walmart, Disney). With each role, Ms. Davis used her influence to lead global initiatives focused on the importance of making risk-informed determinations and engaging all members of the community in the decision-making process. To learn more about The Resiliency Initiative or speak with Ms. Davis, please send an email to info@theresiliencyinitiative.com or visit http://www.theresiliencyinitiative.com.

Get 10x more Visibility across APTs with Red Piranha's SOC-as-a-Service and Crystal Eye

By Adam Bennett, CEO, Red Piranha

Cyberattacks are on the rise and it's crucial for organizations to have a reliable security system that can detect and respond to threats in real-time. Crystal Eye Network Detection and Response (NDR) solution is designed to do just that.

Crystal Eye's integrated platform eliminates the pain of system integration, offering on-demand access to our security professionals via Human-Machine Teaming. This ensures 24x7 protection, detection, and response capabilities.

Additionally, it provides organizations with or without specialists to maintain forensic assurances through real-time threat detection capability using multiple detection methods and supports hunting, forensic and response workflows for best-in-class Threat Detection, Investigation and Response (TDIR).

Deploy Crystal Eye NDR with minimal infrastructure changes, providing a significantly lower Total Cost of Ownership (TCO) with world-class detection technology. Enjoy the benefits of integrated Cyber Threat Intelligence, on-demand Threat Hunting, and response capabilities.

Crystal Eye empowers organizations to identify and respond to network attacks swiftly, preventing significant damage. Its advanced detection capabilities cover a wide range of threats, from malware to ransomware.

The Crystal Eye Advantage

1. Up to 10x Increased Threat Visibility: Gain critical visibility and insight into network operations to deal with APTs and previously unknown attacks through network behavioural analytics.
2. Detect all known Malware families and CnC call outs like Cobalt Strike, for extra assurance.
3. Deploy fully Operationalized and Contextualized Threat Intelligence efficiently and receive Automated Actionable Intelligence to Protect, Detect and Respond to threats proactively.
4. Human-Machine Teaming: Improve incident response and alert prioritization through seamless collaboration.
5. Proactive Threat Hunting: Detect advanced APTs and embedded attacks, reducing dwell time.
6. Multi-Tenanted Sensor Deployment: Deploy a single platform for increased detection engineering, enhancing East-West traffic visibility.
7. Integrated Security PCAP Analysis: Uncover deeper threats and streamline response with Packet Capture (PCAP) analysis.
8. On-Demand SOC Services: Leverage Digital Forensics for rapid response through our SOC services.
9. Advanced Heuristics and ML Anomaly Detection: Ensure alert confidence with cutting-edge Threat Intelligence and contextualization.

Security Operations Centre (SOC) is essential for any organization's cybersecurity strategy. They are technology and dedicated teams of security professionals responsible for monitoring and protecting an organization's networks and systems from cyber threats.

However, setting up and maintaining an in-house SOC can be a complex and expensive proposition and presents its own challenges in an ever-evolving threat landscape. The effectiveness of a SOC is determined by the technology used in operations, risk to those operations as well as the mean time to detect, respond, and recover. In addition, the challenges faced by organizations are driven by people, processes, and technology.

Functions of a Security Operations Center for an organization will vary based on their mission and goals, which are influenced by the organization's risk tolerance, level of security maturity, skills and expertise, processes, and procedures, etc.

What's involved in SOC-as-a-Service?

People

Resourcing skilled professionals has become a significant challenge for organizations, particularly when it comes to building an effective SOC. It is essential to have a broad range of skills such as CISSP, GIAC, GCHI, SANS SEC501, and SANS SEC 503 when it comes to cybersecurity. These include monitoring and analyzing security logs and alerts, as well as being able to identify potential threats and develop strategies to manage them.

Process

An effective SOC relies on meticulous processes, playbooks, and a deep understanding of common and emerging attack scenarios. These processes promptly identify, mitigate, and remediate security incidents. SOC process issues, such as lack of documented escalation and triage processes, can lead to confusion and delays compromising critical systems.

A mature SOC addresses these challenges by implementing a well-defined incident response plan, regularly updating playbooks, and continuously monitoring and evaluating its security posture.

Technology

The lack of interoperability between security tools creates data silo. This results in missed incidents and exploitable blind spots. Integrating and managing multiple technologies is complex, requiring specialized skills and resources not always available in-house.

Effective SOC technology integration requires careful planning and evaluation to ensure seamless interoperability, eliminate blind spots, and streamline security operations.

A true SOC is layered with multiple technology pieces showcasing not limited to Vulnerability Management Solutions, Cyber Threat Intelligence Platforms, Incident Response Capability, SIEM, SOAR, IDPS agents and Log and File transport producing actional alarms in a dashboard.

Red Piranha's SOC-as-a-Service ensures continuous monitoring of your data to detect, prevent, investigate, and respond rapidly to cyber threats with multi-tier 24x7 Eyes on Glass.

With the best-in-breed TDIR, customers get advanced lateral movement and correlation capabilities.

Our customers get cohesive protection against advanced persistent threats (APTs) without the need for new specialist engineering teams, reducing the total cost of ownership for maximum security outcomes.

Crystal Eye consolidates Cloud, Network and End Point Detection with Extended Response.

Crystal Eye's best-in-class monitoring and detection capability, with more than 62,900 IDPS rules updated daily, disrupts the attack chain from all known malware families, including APTs and all complex and modern-day attacks. It also detects initial compromise, persistence, and lateral movement. All of this in a single pane of glass.

Red Piranha's in-house CESOC platform with the following immediate outcomes:

1. Increase traffic and threat visibility across network, cloud and endpoints.
2. Monitoring of the traffic mitigative response, investigation, and containment support.

The functions you want your SOC to include will depend on your organization's specific security needs and risk profile. However, some common functions that most SOCs typically include are:

1. Security monitoring of events and alerts from tools like firewalls, IDS/IPS, antivirus. Continuous eyes-on-glass monitoring of global network activities and system logs.
2. Incident response: Swiftly identify, investigate, and respond to security incidents.
3. Threat intelligence: Stay updated on the latest threats and vulnerabilities that could impact the organization and keep the security team informed about them.
4. Vulnerability management: Identify vulnerabilities in the organization's systems and applications, prioritize them based on their severity, and coordinate with the relevant teams to patch or mitigate them.
5. On-demand digital forensics for investigating security incidents and supporting legal proceedings.

6. Ensure compliance with security regulations and standards.
7. Continuous improvement: Regularly review and enhance organizational processes, tools, and procedures.

Benefits of SOC-as-a-Service

SOC-as-a-Service is a type of Managed Security Service that provides organizations with access to a team of security experts and state-of-the-art technology without the need to set up and maintain an in-house SOC. This can provide several benefits, including:

1. Cost Savings: Outsource SOC operations for substantial cost savings in personnel, training, and technology.
2. Expertise: Access a team of experienced professionals trained in the latest technologies and techniques.
3. Scalability: Scale operations up or down based on evolving threat landscapes without hiring new staff.
4. Continuous Monitoring: Benefit from 24/7 monitoring and support for constant system protection.

Why choose Red Piranha SOC-as-a-Service?

1. Red Piranha is ISO 27001, ISO 9001, and CREST certified.
2. Crystal Eye offers high-fidelity threat detection, investigation, and response.
3. NDR uses ML, analytics, and rule-based matching for anomaly detection.
4. Crystal Eye redefines SOC-as-a-Service, integrating award-winning technology.
5. Turnkey delivery, predefined processes, and a powerful SOAR enhance response capabilities.
6. 24/7 availability for remote response, investigation, and containment by certified experts.
7. Strengthen security with a follow-the-sun approach and 24/7 "Eyes on Glass" capability.

Red Piranha's SOC-as-a-Service provides organizations with effective and cost-efficient ways to protect their networks and systems from cyber threats.

Level up your security maturity backed by a team of security experts working round-the-clock to protect your systems.

About the Author

Adam Bennett is the CEO of the Red Piranha. Adam Bennett is a globally recognised cybersecurity leader, innovator, ethical hacker, and qualified industry expert. As the Founder and Chief Executive Officer, Adam has led Red Piranha from its conception in 2013 to become one of Australia's renowned and awarded cybersecurity organisations. Adam's passion and driving vision is to provide comprehensive cybersecurity protection from the growing threat landscape by offering enterprise-grade cybersecurity solutions to businesses of all sizes.

Prior to founding Red Piranha, Adam accumulated over twenty years of industry experience within the network operations, security, and professional management industries. With over two decades employed within the Security and Risk management industry. Additionally, Adam has enjoyed a long career as a board-level advisor and member on a wide array of public and private organisations, including the WA Cyber Alliance and the Electronic Frontiers Australia as Chairperson of their Business Development Committee.

Adam holds qualifications in Big Data and Social Sciences, Computer Science and Information Security qualifications from Massachusetts Institute of Technology, Charles Sturt University, AMTC; and is a regular lecturer on the topics of network security and encryption. Furthermore, Adam has held varies certifications in Auditing and Cyber security and currently holds certification in CDPSE Certified Data Privacy Solutions Engineer from ISACA. Adam is specialised, trained, and qualified in several disciplines, including but not limited to ethical hacking, digital forensics, risk management, compliance, governance frameworks, cyber laws and project management.

As an industry networker, Adam is a member of several distinct industry groups, including ACS (Australian Computer Society), Foundation member of the Linux Foundation, AISA (Australian Information Security Association), ACSC (Australian Cyber Security Centre), AustCyber and ISACA (Information Systems Audit and Control Association).

A prolific contributor to the IT and Developer industry, Adam is a professional presenter and industry advocate, actively participating within the cybersecurity community industry since the late 1980s. He has authored and contributed to multiple industry papers, including being published with NATO cyber security research, industry research with INTEL and professional blogs, podcasts, amongst other publications.

Adam can be reached online at (info@redpiranha.net) and at our company website https://redpiranha.net

Comparing MDR vs SIEM: Which Is Better for Your Business?

By Vira Shynkaruk, Cybersecurity Content Expert, UnderDefense

Making the right call on cybersecurity solutions is paramount for businesses, especially now, when they are constantly under siege from cyberattacks. The critical decision is MDR or SIEM?

While both solutions offer valuable tools for safeguarding digital assets, understanding their strengths is paramount.

Let's unpack the key differences between MDR and SIEM to understand which shield can best protect your company.

What is SIEM?

SIEM stands for **Security Information and Event Management** and is a powerful **security information gathering and analysis system.**

It provides a comprehensive view of an organization's security posture by centralizing and analyzing data from diverse sources. This enables the security teams to proactively identify potential threats and take necessary measures to mitigate them.

SIEM platforms typically offer data aggregation, log management, event correlation, alerting, and reporting features. They help organizations meet compliance requirements, enhance incident response capabilities, and improve security posture.

Advantages of SIEM

SIEM offers robust advantages that empower organizations to fortify their cybersecurity defenses. Here's a closer look at some of the key benefits:

- **Centralized visibility:** SIEM is a central hub that consolidates security data from various network devices and applications. This unifies your security posture, offering a comprehensive view of potential threats across your IT infrastructure.
- **Enhanced threat detection:** By analyzing the collected data, SIEM can identify anomalies and suspicious activities that might go unnoticed. It helps security teams detect potential threats before they escalate into full-blown attacks.
- **Streamlined log management:** SIEM eliminates the need to sift through logs from individual devices manually. It centralizes log data, making it easier to search, analyze, and identify patterns that could indicate security incidents.
- **Improved Incident Response:** SIEM facilitates faster and more efficient responses to security threats. When an alert is triggered, security personnel have immediate access to relevant data, allowing them to assess the situation and take appropriate action quickly.
- **Compliance adherence:** Many data regulations mandate that organizations retain security logs for a specific period. SIEM provides a centralized repository for security data, ensuring compliance with regulatory requirements.

Disadvantages of SIEM

While SIEM offers significant advantages in threat detection and log management, it also comes with certain limitations:

- **Resource-intensive:** SIEM requires significant computing power and storage capacity to handle the massive amount of data it collects from various sources. This can be a burden for smaller organizations with limited resources.
- **Complexity:** Implementing and maintaining a SIEM system is complex. Effective utilization requires skilled personnel to configure the system, write security rules, and interpret the data generated.
- **False positives:** SIEM relies on pre-defined rules and algorithms to detect threats. Unfortunately, these can sometimes trigger false positives, overwhelming security teams with irrelevant alerts. Sifting through these false alarms takes time and resources from investigating genuine threats.

- **Limited response capabilities:** While SIEM excels at identifying potential threats, it primarily focuses on detection. The system doesn't automatically take action to address them. Security personnel must analyze the data, prioritize alerts, and manually initiate investigations and response measures.
- **Cost:** The cost of SIEM can be a significant factor, especially for larger organizations requiring robust solutions. This includes software licenses, hardware investment, personnel training, and ongoing maintenance.

What Is MDR?

MDR stands for **Managed Detection and Response**. It's a service that provides a **multi-layered defense** against cyberattacks. It provides continuous monitoring, in-depth analysis of security incidents, and automated response capabilities, all backed by a team of security professionals. This approach minimizes the burden on the internal IT team and allows them to focus on core business functions.

Advantages of MDR

MDR provides a high level of protection, combining advanced technology and human expertise. Let's delve into the key advantages that MDR brings to the table:

- **24/7 monitoring and response:** MDR providers offer round-the-clock monitoring and incident response capabilities, ensuring continuous protection, reducing the risk of undetected breaches, and minimizing potential damage to the organization's reputation and finances.
- **Rapid Incident Response:** In a security incident, MDR teams assess the situation quickly, identify the root cause of the breach, and provide rapid response services to contain, investigate, and remediate the threat.
- **Access to expertise and technology:** MDR services leverage a combination of cutting-edge technology, threat intelligence, and skilled security analysts to deliver comprehensive threat detection and response capabilities.
- **Scalability and flexibility:** MDR solutions are scalable and adaptable to the changing needs of organizations, regardless of size or industry. They can easily accommodate growth, expansion, and evolving threat landscapes, providing continuous protection without significant investment in additional resources or infrastructure.
- **Compliance management:** MDR services help organizations meet regulatory compliance requirements by providing detailed reporting and documentation of security incidents and activities.
- **Cost-effectiveness:** MDR solutions offer a cost-effective alternative to building and maintaining an in-house security operations center (SOC). Organizations can reduce operational costs, avoid upfront investments in technology and personnel, and benefit from predictable, subscription-based pricing models by outsourcing security monitoring and incident response to MDR providers.

Disadvantages of MDR

While MDR offers a compelling set of advantages, it also comes with certain limitations that organizations should carefully consider:

- **Cost:** MDR solutions typically involve monthly subscription fees for service, technology, and expertise.
- **Vendor lock-in:** Implementing MDR often requires integrating the provider's security tools with your existing infrastructure. This can create vendor lock-in, making it challenging and costly to switch to a different provider in the future.
- **Limited visibility:** Organizations may cede some control over their security posture as MDR providers manage the detection and response processes. This can lead to reduced visibility into the specific details of identified threats and the actions taken.
- **Potential for reliance:** Overdependence on MDR can lead to a false sense of security. Organizations should not solely rely on the MDR provider and must maintain a basic level of internal security expertise to understand the overall security posture and make informed decisions.
- **Integration challenges:** Integrating MDR solutions with security infrastructure can be complex and require technical expertise. Additional resources may be required to ensure smooth operation and avoid compatibility issues.

Does MDR Include SIEM?

MDR **does not necessarily include SIEM**, but they can work together to provide a more comprehensive security solution. While MDR and SIEM serve distinct purposes, they are complementary and can be integrated to enhance overall threat detection and response capabilities.

- SIEM provides the foundation for threat detection through data aggregation and analysis.
- MDR builds upon this foundation by offering proactive threat hunting, investigation, response, and the expertise of security professionals.

MDR vs SIEM: What Is Better For Your Business?

Choosing between MDR and SIEM depends on your business's needs, objectives, and resources. Here's a comparison to help you determine which is better suited for your organization:

Aspect	MDR	SIEM
Focus	Proactive threat detection and response	Centralized event monitoring and management
Monitoring	24/7 continuous monitoring	Real-time event correlation and analysis
Threat Detection	Proactive threat detection, investigation, and response	Security data aggregation, analysis, and alert generation
Incident Response	Rapid incident response support	Incident investigation and remediation
Security Expertise	Included (security analysts employed by the provider)	Not included
Workload for internal IT team	Reduced	High
Compliance	May assist with compliance requirements	Facilitates compliance management and reporting
Cost	Initial investment with ongoing costs	Significant upfront costs with maintenance expenses
Alert Management	Prioritizes and responds to security alerts	Generates and correlates security events for analysis
Operational Efficiency	Enhances operational efficiency with proactive monitoring	Improves efficiency by automating security processes

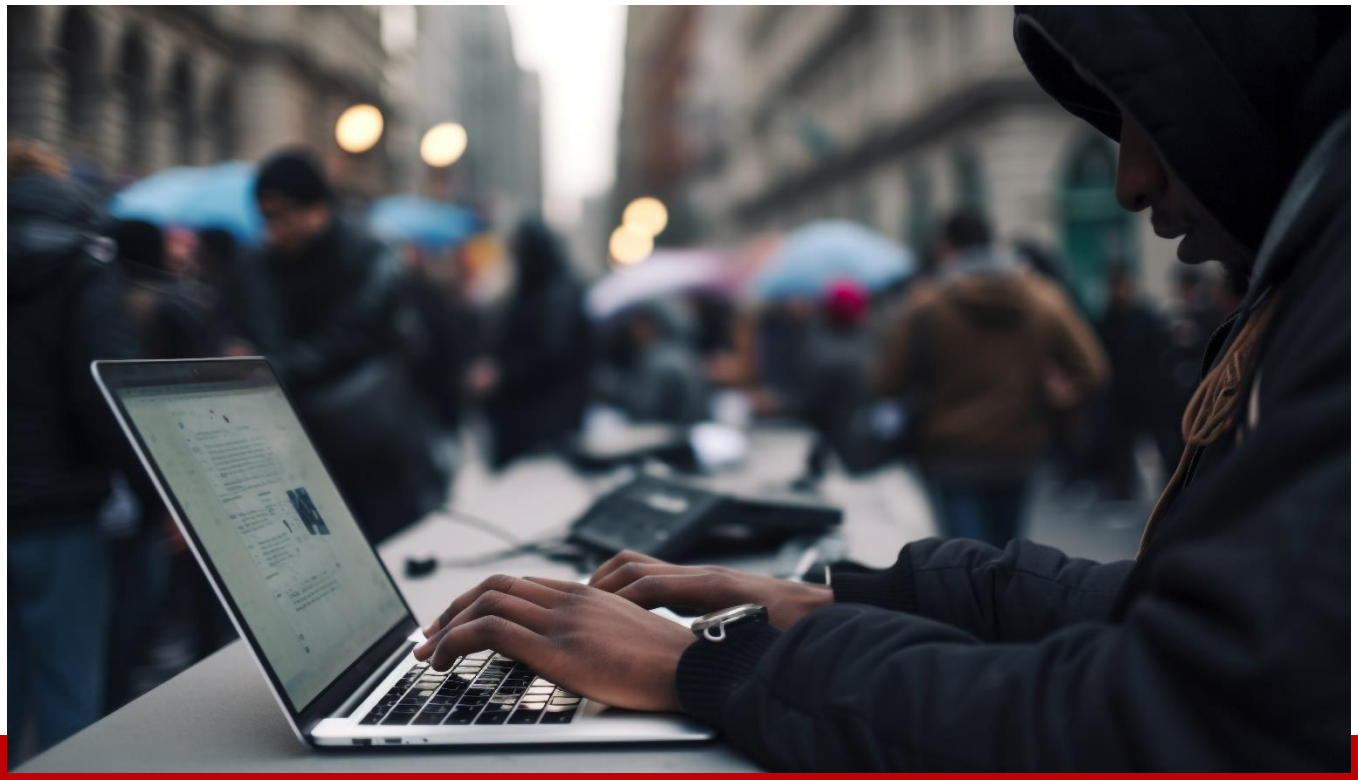
Conclusion

In summary, the choice between MDR and SIEM depends on the organization's security requirements, budget, internal resources, and compliance needs. While MDR offers proactive threat detection and response capabilities, SIEM provides comprehensive visibility and compliance management functionalities. Some organizations may implement MDR and SIEM to effectively leverage each approach's strengths. It's essential to assess your organization's needs and consult with cybersecurity experts to determine the most suitable solution for your business.

About the Author

Vira Shynkaruk is a Cybersecurity Content Expert at UnderDefense.

Vira can be reached online at https://www.linkedin.com/in/vira-shynkaruk-007043145/ and at our company website https://underdefense.com/



Rogue Nations: An Assessment of State-Sponsored Cyberattacks.

By Jacques de la Riviere, CEO, Gatewatcher

Few prefixes excite the cybersecurity market as much as ‘state-sponsored.’

The label immediately conjures images of well-equipped, highly-resourced teams targeting high-profile organisations and individuals. And the war in Ukraine, alongside offensive operations from the likes of North Korea and Iran, has further propelled these images into the public consciousness.

As usual, truth is stranger than fiction: because whilst ‘state-sponsored’ threats are very real and present, they are far more nuanced than one might imagine.

State-sponsored objectives

In this context, "state-sponsored" simply means cyberattacks that are backed by a national government. This does not necessarily mean the government itself is directly responsible for the attacks, but they are providing support or encouragement.

This support may take the form of financial backing, be it funding for attackers or the development of tools. Alternatively, it may be training and resources, or simply offering a combination of sanctuary and cover by ignoring the cyberoperations originating within those borders.

The attacks are linked to the political or economic goals of the 'sponsoring state.' The most common objective is the theft of intellectual property from businesses in a different country, or simply to influence public opinion.

However, in more extreme cases, state-sponsored attacks can aim to disrupt critical infrastructure like power grids or communication systems, or even gain military advantage by stealing information – as cyberattacks become cyberwarfare.

State-sponsored techniques

With such a strong set of resources, state-sponsored groups often have access to a sophisticated arsenal of techniques and tactics. However, when compared to isolated, lone wolf actors, or indeed, small organised criminal gangs, one aspect that characterises state-sponsored groups, is the alignment of these tools to a particular objective.

For example, if espionage or the theft of sensitive data is a primary objective, state-sponsored groups have been seen to use:

- Spear phishing: Crafting emails that appear legitimate, tricking targets into revealing information or clicking malicious links.
- Watering hole attacks: Compromising websites frequented by the target, infecting their computers with malware when they visit.
- Zero-day exploits: Utilizing previously unknown vulnerabilities in software, often acquired through targeted attacks on software developers.
- However, elsewhere, when trying to cripple critical infrastructure, these groups have employed:
- Denial-of-service (DoS) attacks: Flooding a system with traffic, making it inaccessible to legitimate users.
- Malware: Destructive software that can delete data, encrypt files for ransom, or disrupt operations.
- Supply chain attacks: Targeting software providers to inject malicious code into their products, impacting users unknowingly.
- Lastly, there has also been an array of techniques used to influence and manipulate public opinion (typically around political discourse) such as:
- Social engineering: Using social media platforms to spread disinformation, propaganda, or incite unrest.
- Hacking and leaking: Stealing and releasing sensitive information to discredit opponents or sway public opinion.
- Botnets: Networks of compromised devices used to amplify fake news and manipulate online conversations.
- As a mark of the sophistication of the thinking behind these techniques, they are even deployed in different contexts.

Espionage-focused attacks are often long-term campaigns, building trust with targets before extracting information. Attackers typically focus on specific, high-value sectors like defence, energy, or finance.

By comparison, disruption-focused attacks aim for fast, impactful damage. They might target critical infrastructure like power grids or transportation systems during times of heightened tension.

Elsewhere, influencing operations rely on volume. Attackers might manipulate social media algorithms to flood a region with propaganda during an election.

State-sponsored defence

As this brief analysis shows, state-sponsored cyberattacks can pose a major threat. A strategic response is necessary to defend businesses and public sector organisations alike:

Education: Ensuring cybersecurity awareness – and the consequent actions - is vital. Training employees to spot threats and fostering a culture of vigilance are key first steps.

Active defence: Firewalls, network detection and response, intrusion detection, and multi-factor authentication create strong barriers to protect targets.

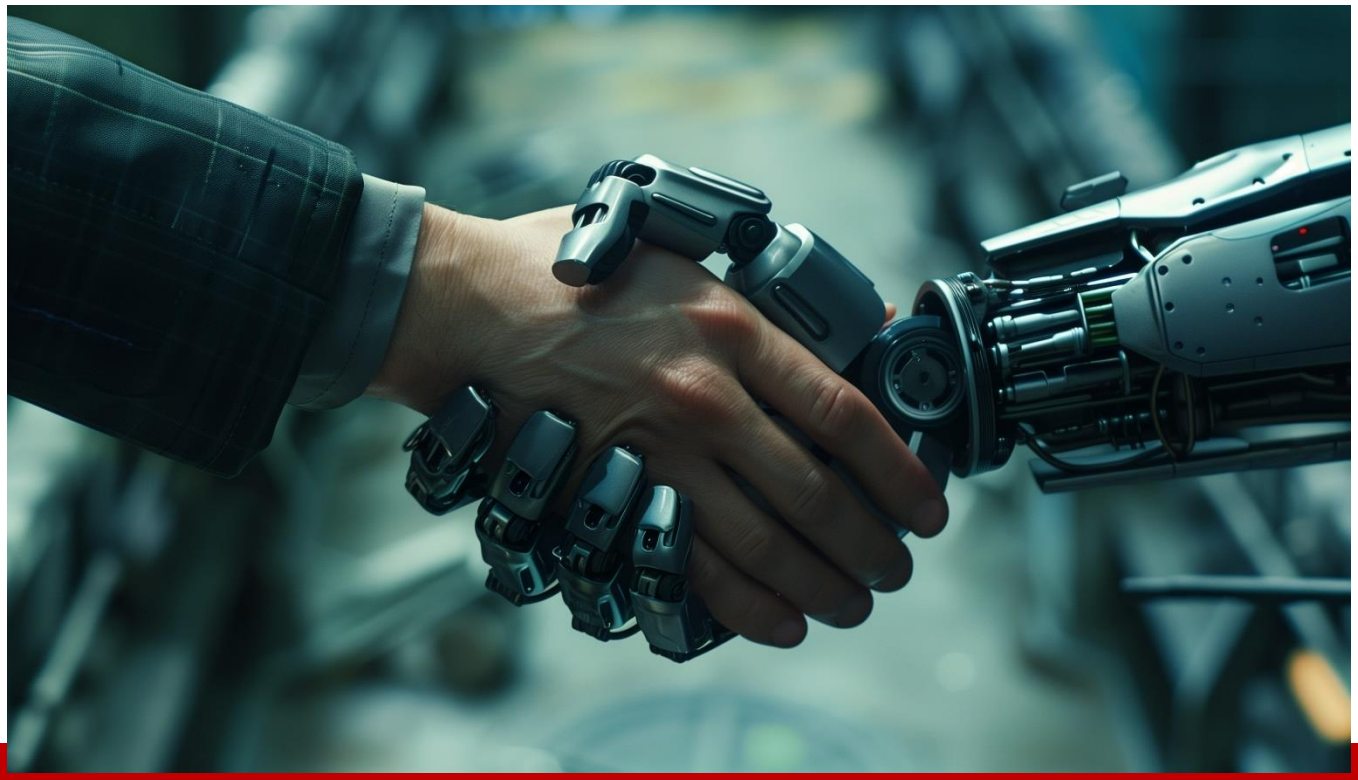
Collaboration: Information sharing means a faster threat identification and a coordinated response. There is strength in numbers.

By understanding the techniques employed and the motivations behind state-sponsored attacks, businesses can empower themselves to protect critical assets in the ever-evolving digital landscape. Whilst it is important to not see these attackers as unbeatable, it is equally important to understand the depth and scope of threat they present.

About the Author

Jacques de la Riviere is the founder and CEO of Gatewatcher, a cybersecurity provider based in France. Jacques has held positions throughout OpenCyber, Adneom and BK Consulting. He is also currently vice-president of Hexatrust - a cluster of 100 European software cybersecurity leaders and cloud providers.

Jacques de la Riviere can be reached online at https://www.hexatrust.com/en/



The AI Arms Race Shaping Federal Cyber Resilience

By Gary Barlet, Federal Chief Technology Officer, Illumio

At its core, the paradox of artificial intelligence (AI) in cybersecurity lies in conflicting uses. On one hand, malicious actors harness AI to launch sophisticated cyberattacks, exploiting vulnerabilities and evading traditional defense mechanisms with alarming efficiency.

Conversely, AI emerges as a powerful ally for defenders, offering advanced analytics and automation capabilities to bolster cyber resilience. AI-driven tools streamline operations by automating routine tasks and facilitating rapid threat detection and response, thus bolstering an agency's ability to mitigate risks effectively. AI can also play a crucial role in securing hybrid environments by dynamically adapting security measures to the complex nature of such infrastructures, ensuring comprehensive protection across on-premises and cloud-based systems.

Machine learning (ML) algorithms, a cornerstone of AI, stand at the vanguard of this defensive revolution. Capable of analyzing vast datasets in real-time, they pinpoint anomalous patterns indicative of potential threats, empowering security teams with timely insights and recommendations.

AI as the Ultimate Defense to Outmaneuver Adversaries

In the ongoing cyber arms race, AI is beginning to emerge as a defense tool to help combat adversaries. By analyzing vast data sets and identifying patterns indicative of potential threats in real-time, AI empowers agencies to proactively detect and neutralize cyber threats before they can inflict harm.

For instance, as a new application comes online, AI can help recognize and auto-label the application. AI might identify it as a customer service application, an internal tool, or a third-party service, depending on the characteristics. Auto-labeling can help write basic rules that would typically require manual intervention to classify the application, segment it within the network, and establish appropriate security rules.

AI's ability to analyze and process information at scale gives defenders a strategic edge, enabling them to anticipate and mitigate emerging threats more effectively than reactive security measures alone. Leveraging predictive analytics and behavioral modeling, agencies can discern subtle indicators of malicious activity and preemptively intervene to thwart attacks before they escalate.

Furthermore, AI-driven threat intelligence platforms empower agencies to aggregate and analyze data from diverse sources, yielding valuable insights into emerging cyber threats and adversary tactics. This comprehensive understanding of the threat landscape enables defenders to adapt their security strategies proactively, closing gaps and fortifying defenses against evolving threats.

The Power of AI and ZTS Working in Tandem

Through rule writing, auto-labeling, and other functions, AI/ML – paired with Zero Trust Segmentation (ZTS), also known as microsegmentation – can quickly and accurately create barriers and compartmentalize networks governed by rigorous authentication protocols. The integration of AL/ML plays a crucial role in Zero Trust frameworks, as these technologies enable continuous monitoring, anomaly detection, and adaptive access controls. Together, they enhance the effectiveness of the Zero Trust model in identifying and mitigating potential security threats in real-time.

ZTS is a foundational capability of Zero Trust that constantly verifies users through the visualization of all communication patterns and traffic between workflows, devices, and internet – allowing agencies to easily see and contain threats in the cloud, data center, network, and endpoints. ZTS protects against any potential threats, unknown actors, or unusual behaviors, so if an attack does occur, the actor cannot easily move throughout the environment and will be prevented from doing further damage.

Today, the convergence of AI and ZTS marks a critical juncture in defense strategies. AI augments ZTS by supporting real-time threat detection capabilities, automating policy enforcement, and enabling adaptive access controls. This symbiotic relationship empowers agencies to confront and neutralize evolving cyber threats, safeguarding critical assets with unprecedented agility and efficacy.

In the increasingly complex landscape of cyber threats, the integration of AI with ZTS also offers a formidable defense strategy. AI can continuously monitor network activities, user behaviors, and system configurations to detect anomalies or suspicious activities in real-time. Meanwhile, ZTS ensures that even

authenticated users are subject to ongoing scrutiny, minimizing the risk of insider threats or unauthorized access.

Powered by ML algorithms, AI undertakes the monumental task of sifting through immense volumes of data in real-time, discerning subtle anomalies that may signify potential security breaches within segmented environments. AI can identify unusual behaviors of a system's peers (who they are talking to) and evaluations of exactly what is happening at the application level (what they are saying). AI solutions are ideally suited for this kind of problem that has multidimensional input and requires multi-dimensional output values that make up system identity.

AI assumes a pivotal role in ZTS frameworks by automating policy enforcement and fostering adaptive access controls. Through continual monitoring and analysis of network traffic, user behavior, and device attributes, AI-driven solutions exhibit a dynamic prowess, capable of adjusting access privileges in response to evolving risk factors.

This seamless integration of AI with ZTS not only enhances the agility and efficacy of cyber defenses but also underscores a proactive stance against emerging threats in today's ever-evolving digital landscape.

The fusion of AI and ZTS presents an effective strategy for reinforcing cyber defenses amidst the ever-changing threat landscape. By integrating AI's sophisticated threat detection capabilities and its capacity to automate policy enforcement, agencies can fortify the foundational principles of ZTS and enhance cyber resilience.

As agencies grapple with the complexities of the cyber realm, harnessing AI as the ultimate defense tool empowers them to not only thwart adversaries, but also to maintain a strategic advantage in the ongoing cyber arms race. Despite the evolving landscape of cyber threats driven by emerging technologies utilized by attackers, agencies can harness these very technologies to fortify their resilience and security posture, enabling them to adeptly navigate this dynamic and relentless realm of cybersecurity.

About the Author

Gary Barlet is the Federal Chief Technology Officer at Illumio, where he is responsible for working with government agencies, contractors and the broader ecosystem to build in Zero Trust Segmentation as a strategic component of the government Zero Trust architecture. Previously, Gary served as the Chief Information Officer (CIO) for the Office of the Inspector General, United States Postal Service. He has held key positions on several CIO staffs, including the Chief of Ground Networks for the Air Force CIO and Chief of Networks for the Air National Guard CIO, where he was responsible for information technology policy and providing technical expertise to senior leadership. He is a retired Lieutenant Colonel from the United States Air Force, where he served as a Cyberspace Operations Officer for 20 years. Gary can be reached online at https://www.linkedin.com/in/gary-barlet-4384115/ and at our company website https://www.illumio.com/

Is Your Organization a Laggard or a Leader in Digital Trust?

By Mike Fleck, Head of Product Marketing at DigiCert

Digital trust is at the core of what makes internet connected experiences valuable. Whether we're making an e-commerce purchase, signing a legal document, or pairing our phone to a glucose monitor, we need to be certain that the people and devices we're interacting with are legitimate. We also need peace of mind in knowing that those interactions remain secure.

Business decision-makers understand that digital trust is fundamental to today's business processes. As new security threats and emerging technologies like AI and deepfakes threaten to undermine trust, it's even more important that organizations work proactively to maintain trust across all their communications and supply chains.

To gain a deeper perspective into how well enterprise organizations are succeeding, DigiCert conducted a new State of Digital Trust survey in 2024. Eleven Research of Dallas, Texas, surveyed 300 senior decision makers in small to large enterprises throughout EMEA, North America, and APJ. The report explored some of the key drivers of interest in digital trust, asked organizations to evaluate their progress, and took a close look at the success and challenges of specific trust initiatives.

Digital trust remains top of mind

The State of Digital Trust survey sought to determine why enterprises remain so focused on digital trust. The most important drivers included:

- The emergence of more remote workers as part of today's increasingly hybrid workforce
- More networks, including additional devices at the network edge connecting to partners and customers
- Escalating customer expectations for digital trust

Survey participants also cited drivers like the increasing pace of business; increasing threat surface, escalating network and application complexity; and growing threats from bad actors and exploits.

Despite their understanding of the need for digital trust, organizations still contend with real challenges in achieving it. Many face a lack of staff expertise, since not all staff have the expertise needed to govern digital trust in a centralized, scalable way given the many stakeholders involved.

The scope of what enterprises need to protect is also daunting, as the number of connected users and digital assets grows. Organizations also cited a lack of management support, as the economic environment has become more challenging, and resources are more limited.

How well are organizations doing?

Although the new survey showed that most enterprises are fully engaged with the digital trust issue, their success varied, depending on certain areas of focus. To better understand the differences between digital trust "leaders" compared to "laggards," the survey also tiered the results, and compared organizations based on their responses.

Enterprise trust practices

Enterprise digital trust is usually managed by IT, and includes initiatives like certificate management, identity and access management, and endpoint or email security. Most enterprises have had these initiatives in place for years, so it was surprising that only 1 in 100 enterprises describe their enterprise digital trust practices as "very mature."

More than 90 percent reported outages, brownouts, and data breaches, while most reported limited agility to respond to outages and security incidents. However, organizations identified as digital trust leaders performed much better. These organizations exhibited fewer issues related to enterprise trust, with no outages, few data breaches, and no compliance or legal issues.

IoT and connected device trust practices

This category focused on companies that that sell or manufacture IoT devices such as factory sensors, home thermostats, and smart watches. Like enterprise organizations, most of these manufacturers were doing well, but not great.

Surprisingly, 87% reported that they exchange personal information from IoT and connected devices via non-encrypted channels. But once again, digital trust leaders performed better than laggards, reporting no compliance issues related to connected and IoT device trust.

Software trust

The survey also examined how well organizations were ensuring digital trust for the software that they sell or distribute to end customers. Nearly all (99%) reported that they were code signing software source code. However, only one third code-signed environments such as containers.

Although these practices are a great start, just one in 20 rated their enterprise trust practices as extremely mature. None reported that they would be able discover all applications for a specific code-signing private key, in the event it was compromised. Among digital trust leaders, fewer digital trust issues were reported. None of the top organizations reported experiencing compliance issues or software supply chain compromises.

ESignature trust

ESignature trust practices received the lowest rating out of the areas surveyed. Approximately half of participants used electronic seals for sales, procurement, payroll, and legal documents. This category also showed a high incidence of problems related to digital document trust issues, with 100% reporting issues with identity theft or impersonation, problems with paper-based contract processes, and bad actors misrepresenting a document as coming from their organization.

However, especially among digital trust leaders, eSignature trust practices have helped organizations with digital innovation, employee productivity, and brand reputation.

Taking a proactive approach to trust

As the importance of digital trust grows, the gap between organizations that are successful at managing, and those that are falling behind, is growing as well. Most digital trust leaders and laggards are already aware of where they stand. However, the risk comes into play when organizations may be unaware of their limitations.

What steps can you take to gain better self-awareness when it comes to digital trust, and put an effective strategy in place?

Take inventory

The first step in managing digital trust is gaining visibility and insight into the parts of your business that most depend on it. Take a close look at the processes that rely on digital trust, and understand how your organization protects, uses, and manages digital identities, cryptographic keys, and related assets. You can do the inventory manually, or save time by automating the processes, using technology tools to scan your systems and/or ingest data from your IT asset management systems and other resources.

Understand and define your processes

Once you've acquired a strong understanding of your digital trust processes, you can build or strengthen policies to support them more effectively and align them to your specific needs. A good place to start is with foundational policies for trust, covering areas like cryptography and public key infrastructure. Then you can zero in on processes and tools that need more specific attention.

Optimize PKI management

Achieving crypto-agility is key to a proactive approach to future threats. Centralizing policy enforcement and automating management of cryptographic assets can make it easier to update cryptographic assets at scale or mitigate issues more quickly. A centralized approach to managing digital assets and certificates can also help you gain visibility, ease administration, and bring risk down.

Next steps

We've already seen the need for digital trust across a variety of industries, and its importance will only grow. Regardless of where you are in your adoption of digital trust, it's important to keep pace with new threats, new digital business processes—and new opportunities. With a forward-looking strategy, you can position your organization to meet today's changing needs, as well as tomorrow's.

About the Author

Mike Fleck is Head of Product Marketing at DigiCert. He has more than 25 years of cybersecurity industry experience across network security, data encryption, threat intelligence, malware analysis, identity protection and e-mail security, and holds a patent for transparent data encryption.

Mike can be reached online at https://www.linkedin.com/in/mfleckca/ and at our company website https://www.digicert.com/

Strengthening Cybersecurity

Transforming in the Age of Healthcare Digitalization

By Brian White, Co-Founder of DoorSpace

Healthcare and technology increasingly intersect in today's world, and cybersecurity has become a primary concern for many companies. However, the recent attack on Change Healthcare serves as a harsh reminder of the vulnerabilities facing the healthcare sector. Most healthcare organizations, from small clinics to major hospitals, face significant risks. It's not a question of if, but when a major breach will occur. As healthcare continues to integrate more deeply with digital technologies, the imperative to bolster cybersecurity measures has never been more urgent.

Understanding the Risks

It is no secret that healthcare organizations hold a lot of sensitive data, including personal health information (PHI), payment details, and personal identification numbers; not to mention the particularly vulnerable information of the workers themselves. This makes healthcare organizations prime, and sometimes vulnerable, targets for cyberattacks. The ramifications of such breaches are severe, ranging from financial loss to significant reputational damage, and most critically, risks to patient safety.

The digitalization of healthcare, while offering benefits like improved patient care and operational efficiency, also multiplies the points of vulnerability. Electronic Health Records (EHRs), telemedicine, mobile health applications, and automated pharmacy dispensing systems are just a few examples of technologies that, if compromised, could lead to increased vulnerability.

The breach at Change Healthcare is not isolated. Several high-profile attacks in recent years have underscored the susceptibility of the healthcare industry. For instance, ransomware attacks have locked healthcare providers out of crucial systems, delayed surgeries, and even forced hospitals to revert to paper records. Data breaches have exposed millions of patient records, leading to identity theft and fraud.

To combat the escalating cyber threats, healthcare organizations must adopt a comprehensive and layered approach to cybersecurity. This strategy should begin with risk assessment and management, where regular evaluations are conducted to identify and prioritize vulnerabilities within the system. Alongside this, robust data governance and management policies need to be implemented to safeguard sensitive information.

The adoption of advanced security technologies is also vital. By utilizing cutting-edge tools such as artificial intelligence (AI) and machine learning (ML), organizations can detect and respond to threats in real time. Additionally, the use of encryption and secure access protocols is crucial to protect the integrity and confidentiality of patient data.

Employee training and awareness play a critical role in cybersecurity. Healthcare organizations should conduct regular training programs to keep staff updated on the latest cyber threats and preventive practices. Cultivating a culture of security within the organization empowers employees to take an active role in protecting sensitive information.

Incident response planning is another essential element. Organizations need to develop and regularly update their incident response plans to ensure they can act quickly and effectively in the event of a breach. Simulating cyberattack scenarios helps prepare and refine response strategies, ensuring that staff are ready to handle real incidents efficiently.

The Role of Leadership in Cybersecurity

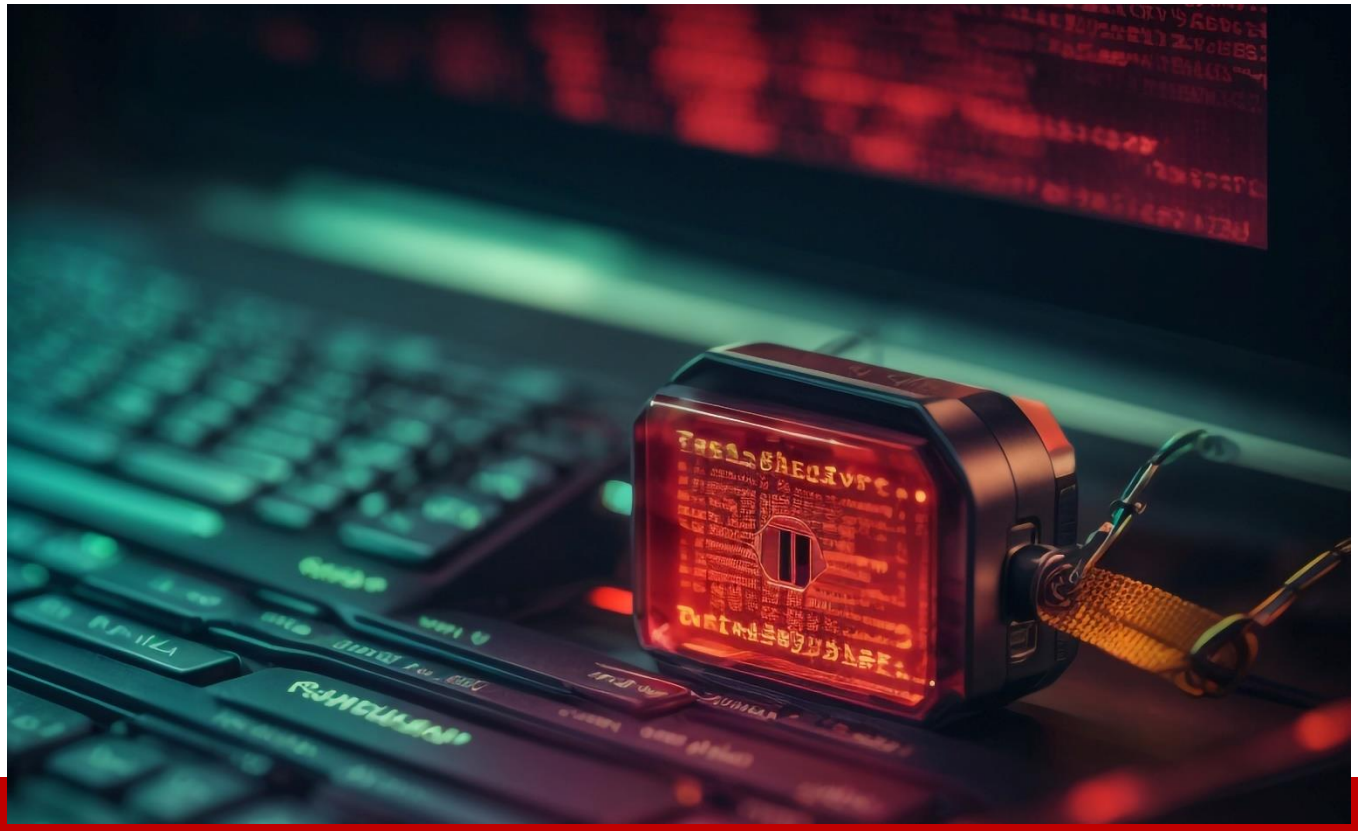
Leadership plays a crucial role in fostering a secure environment. Executives must prioritize cybersecurity, allocate appropriate resources, and advocate for a continuous improvement approach to security practices. Leadership commitment not only enhances security but also builds trust among patients and stakeholders. It's no longer good enough for the C-Suite in hospitals to rely on the IT department for guidance. Cybersecurity needs to be led from the top.

The digital revolution in healthcare presents both opportunities and challenges. While technology can dramatically improve healthcare delivery, it also introduces significant security risks. By adopting a comprehensive and proactive approach to cybersecurity, healthcare organizations can protect themselves against the growing threat of cyber-attacks. The goal is clear: to ensure that digital advancements in healthcare translate into safer, more effective patient care without compromising security and privacy.

About Brian White

Brian White is the CRO and Co-founder of DoorSpace. He has 14 years of experience in business development and B2B software sales helping organizations leverage technology to add efficiency, drive revenue growth and improve their customer experience.

Brian White can be reached online at https://doorspaceinc.com/



The Scourge of Ransomware

By Jaye Tillson, Director of Strategy and Field CTO, Axis Security / HPE

Ransomware has become a growing threat in our new hybrid world. It encrypts a victim's files, rendering them inaccessible, and demands a ransom payment for the decryption key. This can cripple businesses, government agencies, and even individuals, causing significant financial losses, operational disruptions, and reputational damage.

How Ransomware Works:

Ransomware typically infiltrates a system through phishing emails, malicious software downloads, or network security vulnerabilities. Once inside, it encrypts files, making them unusable. Hackers then demand a ransom payment, usually in cryptocurrency, to provide the decryption key. The pressure is high, as victims risk losing access to critical data permanently if they don't comply.

Ransomware Attacks 2021-2024:

While the exact ransom amounts paid are often not publicly disclosed, here are five significant ransomware attacks that have hit headlines in the last three years:

1. **MOVEit Attack (May 2023):** The CL0P ransomware group exploited a vulnerability in MOVEit, a popular file transfer software. This attack impacted numerous high-profile companies, including the BBC, British Airways, and Ernst and Young, causing major disruptions. The ransom demands and total amount paid remain undisclosed.

2. **Colonial Pipeline Attack (May 2021):** This attack targeted a critical piece of US infrastructure - the Colonial Pipeline, which transports gasoline and diesel fuel across the East Coast. Using DarkSide ransomware, the attackers forced the pipeline to shut down for several days, causing fuel shortages and panic buying. Colonial Pipeline reportedly paid a ransom of $4 million.

3. **Kaseya Supply Chain Attack (July 2021):** REvil ransomware exploited a vulnerability in Kaseya VSA, a remote monitoring and management software used by Managed Service Providers (MSPs). This attack rippled through the supply chain, impacting thousands of businesses that relied on MSPs for IT support. The estimated ransom demands exceeded over $70 million, though the amount paid is unknown.

4. **Costa Rica Government Attack (April 2022):** The Conti ransomware group launched a large-scale attack on Costa Rica's government systems, crippling critical services like tax collection and social security. The government refused to pay the ransom demands, opting for data restoration efforts.

5. **Hollywood Presbyterian Medical Center Attack (February 2023):** This attack, using the LockBit ransomware strain, disrupted operations at the medical center, forcing them to delay surgeries and appointments. The attackers demanded a ransom of $34 million, but the hospital's response and the amount paid are undisclosed.

The Fight Against Ransomware: Introducing Zero Trust

Combating ransomware requires a multi-pronged approach. Businesses need robust cybersecurity measures like data backups, user education, and endpoint protection. Governments are collaborating to disrupt ransomware operations and international law enforcement is working to track down perpetrators. There's growing awareness about the importance of not paying ransoms, as it incentivizes further attacks.

One increasingly important defense strategy is **Zero Trust**. This security model assumes no user or device is inherently trustworthy, constantly verifying them before granting them access to resources. Here's how Zero Trust can specifically help against ransomware attacks:

- **Limiting Lateral Movement:** Ransomware often spreads within a network after gaining an initial foothold. Zero Trust's micro-segmentation restricts access to specific resources, making it difficult for ransomware to move laterally and encrypt vast amounts of data.

- **Least Privilege Access:** Zero Trust enforces the principle of least privilege, granting users only the minimum access level required for their tasks. This reduces the potential damage if a compromised account is exploited by ransomware.
- **Continuous Monitoring:** Zero Trust involves constant monitoring of user activity and system behavior. This allows for early detection of suspicious activity, potentially stopping a ransomware attack before significant encryption occurs.
- **Stronger Identity Verification:** Multi-factor authentication and other strong verification methods make it harder for attackers with stolen credentials to bypass security measures.

Conclusion

Organizations can significantly reduce the risk and impact of ransomware attacks by implementing Zero Trust principles. However, Zero Trust is not a silver bullet. It should be layered with other security measures to create a comprehensive defense strategy.

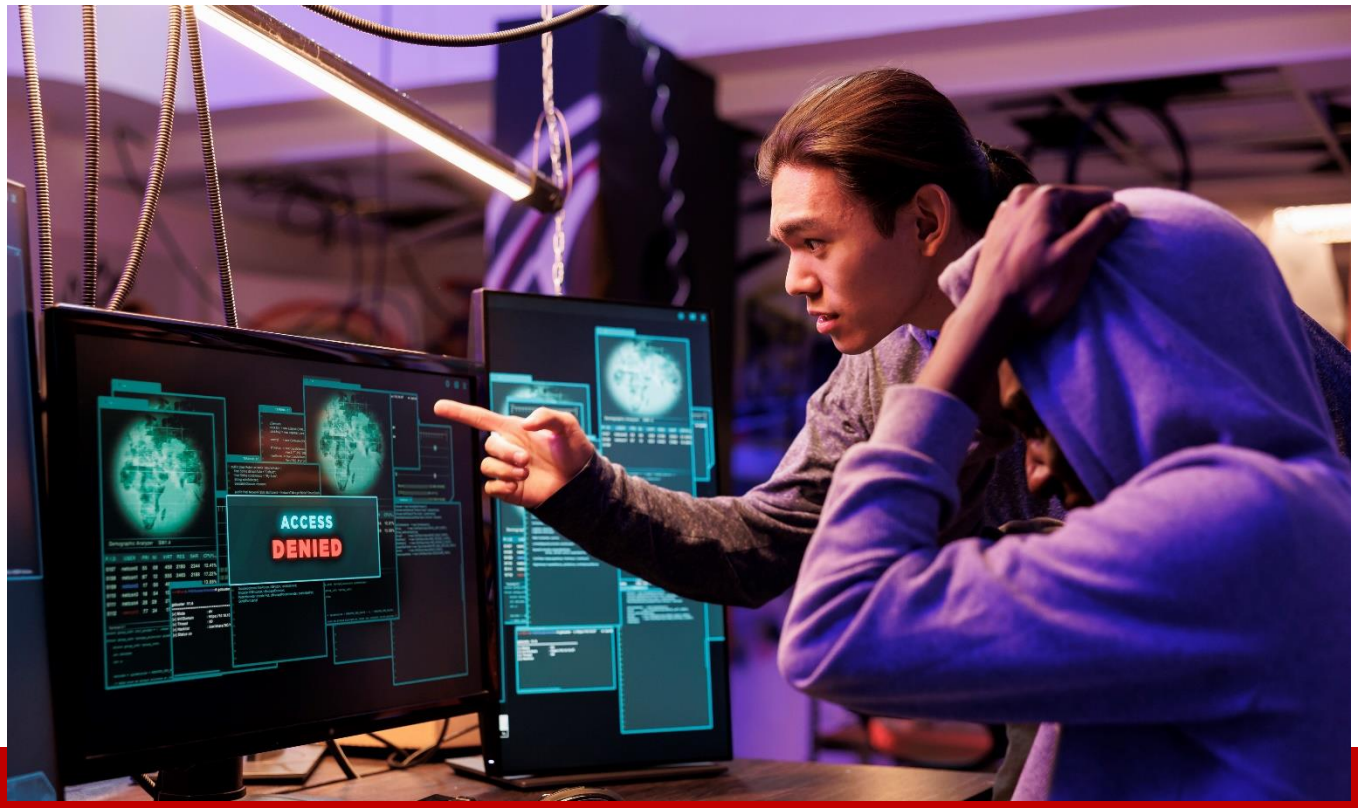
About the Author

Jaye Tillson is Director of Strategy and Field CTO at Axis Security (acquired by HPE), boasting over 25 years of invaluable expertise in successfully implementing strategic global technology programs. With a strong focus on digital transformation, Jaye has been instrumental in guiding numerous organizations through their zero-trust journey, enabling them to thrive in the ever-evolving digital landscape.

Jaye's passion lies in collaborating with enterprises, assisting them in their strategic pursuit of zero trust. He takes pride in leveraging his real-world experience to address critical issues and challenges faced by these businesses.

Beyond his professional pursuits, Jaye co-founded the SSE Forum and co-hosts its popular podcast called 'The Edge.' This platform allows him to engage with a broader audience, fostering meaningful discussions on industry trends and innovations.

Jaye Tillson can be reached online at https://www.hpe.com/us/en/products.html



AI and Cybersecurity: Mitigating Risks and Safeguarding Digital Assets

Leveraging Artificial Intelligence to Enhance Cybersecurity Defenses

By Harish Mandadi, CEO and Founder, AiFA Labs

AI and Cybersecurity: Mitigating Risks and Safeguarding Digital Assets

Artificial Intelligence has become essential for safeguarding digital resources in cybersecurity. As organizations strive to defend against pragmatic threats, AI offers crucial risk reduction and defense reinforcement. Let's explore the integration of AI in cybersecurity, focusing on its significance, applications, and impact on safeguarding digital assets.

What does AI do for security?

AI improves security by analyzing data for unusual patterns and behaviors, enabling early threat detection and real-time monitoring for swift response to potential threats.

Additionally, AI helps automate and streamline incident response, reducing the time and resources required to respond to threats. It also identifies vulnerabilities, predicts conceivable threats, and improves security incident response.

Utilizing AI in Cybersecurity

AI plays a crucial role in cybersecurity by monitoring and analyzing behavior patterns to establish a baseline, enabling the detection of unusual activities and restriction of unauthorized access to systems.

It prevents threats from materializing by facilitating risk prioritization, rapid detection of potential malware and intrusions, and proactive measures to prevent threats from materializing. Explore how proper utilization of AI will enhance your cybersecurity system, mitigating potential security risks.

Real-Time Threat Detection with AI

Real-time threat detection with AI transforms cybersecurity practices. By employing machine learning and advanced analytics, AI systems promptly identify and address threats, minimizing the likelihood of security breaches and limiting their impact.

This proactive approach empowers organizations to anticipate emerging threats, safeguard sensitive data, and maintain uninterrupted operations. AI-driven real-time threat detection excels in accuracy and speed, scrutinizing extensive data sets to detect even subtle anomalies.

Consequently, security teams can react swiftly and efficiently, reducing the mean time to detect (MTTD) and the mean time to respond (MTTR). Integrating AI into cybersecurity strategies fortifies defenses, mitigates risks, and secures digital assets amidst the ever-changing threat landscape.

Predictive Analytics for Enhanced Security

Predictive analytics is a crucial element of AI-driven cybersecurity, aiding organizations in anticipating and preparing for potential security breaches. By examining historical data, external intelligence, and real-time threat feeds, predictive analytics helps pinpoint vulnerabilities and predict potential attacks.

This proactive approach empowers security teams to take preemptive actions, bolstering defenses and minimizing the likelihood of a successful breach. The advantages of predictive analytics in cybersecurity are evident. Organizations can optimize their security resources and enhance incident response capabilities by identifying high-risk areas and anticipating attack vectors.

Moreover, predictive analytics enables organizations to remain ahead of emerging threats, reducing the risk of security breaches and safeguarding sensitive data. By integrating predictive analytics into cybersecurity strategies, organizations can elevate their security posture, protect digital assets, and mitigate the threat of cyber attacks.

Automated Response Systems

Automated Response Systems (ARS) play a pivotal role in AI-driven cybersecurity, enabling organizations to swiftly and efficiently address security threats. Leveraging AI algorithms, ARS analyzes threat data, detects patterns, and triggers automated responses to contain and mitigate attacks.

This rapid response capability significantly reduces the mean time to respond (MTTR) and mitigates the impact of security breaches. ARS seamlessly integrates with other AI-powered cybersecurity tools, such as predictive analytics and threat detection systems, to establish a comprehensive security framework.

By automating incident response processes, organizations can allocate more time for strategic initiatives, enhance incident response efficiency, and minimize the risk of human error. With ARS in place, organizations can respond to security threats in real time, ensuring the protection of sensitive data and the safeguarding of digital assets.

AI-Powered Breach Detection Systems

AI-powered breach Detection Systems are an advanced solution in combating cyber threats, utilizing artificial intelligence and machine learning for real-time identification and response to security breaches.

These systems analyze network traffic, system behavior, and user activity to detect anomalies and patterns signaling a breach, enabling prompt and efficient incident response. They excel in identifying threats overlooked by traditional security measures, thus lowering the risk of security breaches and safeguarding sensitive data.

Breach detection systems continuously adapt to evolving threats, enhancing detection accuracy using AI and machine learning. They facilitate swift and effective response actions, thereby minimizing the impact of security breaches.

With AI-powered breach detection systems, organizations fortify their security stance, mitigate risks, and protect digital assets. These systems constitute a vital element of a comprehensive cybersecurity strategy, empowering organizations to address emerging threats and defend against cyber-attacks.

Enhanced Phishing Detection

Enhanced phishing detection is a vital element of modern cybersecurity, shielding organizations from the escalating threat of phishing attacks. By scrutinizing email patterns, sender behavior, and content, AI algorithms discern potential phishing attempts, flag suspicious emails, and thwart employees from falling prey to such attacks.

This detection capability significantly diminishes the risk of security breaches, financial loss, and reputational harm. These AI-powered phishing detection systems continuously evolve and adapt to unexplored phishing tactics, enhancing detection accuracy and preempting emerging threats.

These systems create an impenetrable defense against phishing attacks, safeguarding sensitive data and preserving digital assets integrated with other cybersecurity tools. With Enhanced Phishing Detection, organizations empower their employees to make informed decisions, mitigate the risk of human error, and fortify their overall cybersecurity posture.

User Behavior Analysis

User Behavior Analysis (UBA) is a state-of-the-art cybersecurity method that utilizes AI to monitor and analyze user behavior, swiftly identifying potential security threats. Through scrutinizing patterns of user activity, UBA detects anomalies and deviations from normal behavior, effectively flagging potential security risks and thwarting insider threats.

This approach enables organizations to proactively address emerging threats, reducing the risk of security breaches and safeguarding sensitive data. AI-powered UBA systems continuously learn and adapt to user behavior, enhancing detection accuracy while minimizing false positives.

UBA offers a comprehensive security framework integrated with other cybersecurity tools, enabling organizations to respond promptly and efficiently to security incidents. With UBA in place, organizations can effectively identify and mitigate insider threats, thereby protecting digital assets and preserving their reputation. By analyzing user behavior, UBA provides a critical layer of defense in the ongoing battle against cyber threats.

AI has transformed the cybersecurity industry, providing exceptional threat detection, incident response, and predictive analytics capabilities. Organizations can now safeguard digital assets more effectively through AI integration and solutions.

About the Author

As CEO and Founder of AiFA Labs, I spearhead a team of cybersecurity experts providing cutting-edge solutions to safeguard clients across various industries. With over 20 years of experience in IT sales and delivery, I bring a unique blend of entrepreneurial vision and hands-on technical expertise to the dynamic landscape of cybersecurity. My mission is to empower organizations with innovative solutions to stay ahead of evolving threats and protect their digital assets

Harish Mandadi (LinkedIn: https://www.linkedin.com/in/harish-mandadi-a3154016/)

Website: https://www.aifalabs.com/

Optimizing IT Team Collaboration

An Innovative Approach to Enhancing Productivity

By Juan Betancourt, CEO, Humantelligence

Optimizing IT team collaboration hinges on recognizing their unique team challenges, such as siloed knowledge and communication barriers, as well as the different working styles of product managers, software engineers, data scientists, and architects. Given the outsourced and gig economy nature of IT, many of these people find themselves having to collaborate across different offices, time zones, and regions – resulting in cultural and communication differences that lead to even more complexity when it comes to practicing effective collaboration.

An innovative approach encourages understanding diverse team dynamics and leveraging them for enhanced productivity. This method goes beyond traditional strategies by advocating for tailored communication and problem-solving tactics. It drives improvements in teamwork and efficiency, offering substantial insights into maximizing the potential of IT professionals and their collaborative endeavors.

Deep Dive into Team Dynamics and Self-Awareness

The Impact of Self-Awareness on Team Effectiveness

When team members are self-aware, they communicate better, adapt quickly, and contribute more effectively to their team's success. Here's how you can enhance self-awareness in your team:

1. **360-Degree Feedback:** Team members receive confidential, anonymous feedback from peers, subordinates, and supervisors. This comprehensive view helps individuals understand how their behavior affects others, encouraging personal development and team cohesion.
2. **Personality Assessments:** Utilize tools to understand all the dimensions of personality types and how these behaviors, motivators, and work energizers shape a team member. These assessments also reveal how individual traits contribute to team dynamics and inform how to interact more effectively.
3. **Mindfulness Practices:** Engage in regular mindfulness or meditation exercises. This can increase emotional intelligence, helping individuals respond to workplace stressors more calmly and thoughtfully.
4. **Journaling:** Encourage daily reflection through journaling. This practice can uncover patterns in thought and behavior, enhancing personal growth and understanding of how one's actions affect the team.
5. **Role-Playing Scenarios:** Simulate challenging communication or problem-solving scenarios. Role-playing can help team members anticipate reactions, understand different perspectives, and improve empathy.

Understanding and Appreciating Diverse Work Styles

Recognizing and valuing diverse work styles within IT teams leads to more effective collaboration, innovative solutions, and a more inclusive work environment, all contributing to enhanced productivity.

Strategies for fostering appreciation and synergy:

1. **Regular Team-Building Activities:** Engage in activities that highlight individual strengths and promote understanding. For instance, problem-solving games can show diverse approaches and solutions from different work styles.
2. **Open Forums for Sharing:** Hold regular meetings where team members share their working styles and preferences. This transparency builds respect and enables better planning and task allocation.
3. **Cross-Training Sessions:** Rotate roles or conduct workshops where team members can experience and appreciate the challenges and skills involved in different roles within the team.
4. **Recognition Programs:** Implement systems to acknowledge and celebrate the contributions of all work styles. This could be through awards, shoutouts, or showcasing successful projects and the diverse methods used.
5. **Conflict Resolution Training:** Equip the team with the skills to navigate disagreements constructively. Understanding how to communicate and compromise with different work styles prevents conflicts and enhances collaboration.

Communication as a Foundation for Team Success

Overcoming Communication Barriers

Effective communication is the bedrock of team success, especially in IT where complex ideas and projects are the norm. Enhancing dialogue removes barriers, leading to quicker problem-solving and innovative solutions.

Common communication challenges in IT environments:

1. **Technical Jargon:** Simplify language. Here's an oversimplified example: Instead of saying "Implement a robust SSO protocol," say "Let's make signing in easier and more secure for everyone."
2. **Virtual Miscommunications:** Use video calls to ensure nuances aren't lost. For instance, discussing complex issues face-to-face (virtually via video meetings) instead of lengthy email threads.
3. **Cultural Differences:** Acknowledge and embrace diverse communication styles. For example, understanding and respecting that some cultures are more direct while others are more indirect in their communication.
4. **Information Overload:** Prioritize and condense information. Turn a 10-point email into a concise 3-point action list with clear objectives.

Practical tips for improving clarity and understanding in team communication:

1. **Regular Team Check-Ins:** Short, daily meetings can keep everyone aligned on tasks and reduce misunderstandings.
2. **Active Listening Workshops**: Training in active listening improves empathy and understanding among team members.
3. **Feedback Culture:** Encouraging constructive feedback helps identify and rectify communication issues quickly.
4. **Utilizing Collaboration Tools:** Tools like Slack or Trello that can integrate with specialized collaboration plug-ins to streamline communication and keep track of conversations and decisions.

Building a Culture of Openness and Trust

A communicative environment leads to better problem-solving, stronger relationships, and a more agile response to challenges.

Methods for creating an environment where team members feel safe to express ideas and concerns:

1. **Regular Open Forums:** Hold meetings where team members can discuss anything, from project updates to personal concerns, ensuring everyone's voice is heard.

2. **Anonymous Feedback Systems:** Implement a platform where employees can share their thoughts and suggestions anonymously, encouraging more honest and constructive feedback.
3. **Team Charters:** Create a team agreement that outlines how members should communicate, resolve conflicts, and support each other, reinforcing a shared commitment to openness.
4. **Conflict Resolution Mechanisms:** Establish clear processes for addressing and resolving conflicts, demonstrating that all concerns are taken seriously and managed respectfully.
5. **Recognition of Contributions:** Regularly acknowledge and celebrate successes and contributions from all team members, fostering a positive and inclusive atmosphere.

Aligning Individual Strengths with Team Goals

Effective Role Allocation and Flexibility

Effective role allocation and flexibility in IT teams enhances team synergy, accelerates project completion, and fosters a dynamic environment where adaptability is a strength.

Techniques for aligning individual strengths with team roles and projects:

1. **Strengths-Based Assignments:** Utilize assessments to understand each member's top strengths, then assign roles and tasks that align with these attributes for increased engagement and effectiveness.
2. **Rotational Programs:** Implement rotational assignments that allow team members to explore different roles and projects, fostering a deeper understanding of various functions and identifying best-fit scenarios.
3. **Task Ownership Opportunities:** Encourage team members to take ownership of tasks or projects they feel passionate about or have a particular skill set for, enhancing motivation and quality of work.
4. **Continuous Learning & Development:** Foster a culture of ongoing education where team members are encouraged to develop new skills and apply them to different aspects of projects, thus adapting to changing demands and expanding team capability.

Encouraging Skill Development and Growth

Encouraging skill development and growth not only improves team capability and adaptability but also boosts morale and retention by investing in each member's professional journey.

Strategies for continuous skill development within the team:

1. **Personalized Learning Plans:** Craft individual learning paths based on each member's career aspirations and the team's needs, including certifications, courses, and workshops relevant to emerging technologies.
2. **Mentoring and Coaching:** Pair less experienced members with seasoned professionals for knowledge sharing, guidance, and support, encouraging a continuous flow of learning within the team.

3. **Project-Based Learning:** Encourage learning by doing, where team members can apply new skills to real-world projects, allowing them to tackle new challenges and learn from the outcomes in a supportive environment.
4. **Regular Skill Audits:** Periodically review the team's skill sets and identify gaps or areas for improvement, ensuring that training and development are targeted and effective.

Decision Making and Conflict Resolution in IT Teams

Inclusive Decision-Making Processes

Inclusive decision-making in IT teams enhances solution quality and buy-in by incorporating diverse perspectives and expertise. It mitigates risks, fosters innovation, and ensures that decisions reflect collective intelligence, leading to more effective and sustainable outcomes.

Methods for ensuring all voices are heard in decision making:

1. **Round Robin Technique:** During meetings, give each team member a chance to voice their opinion or suggestion on the matter at hand, ensuring everyone has the opportunity to contribute.
2. **Anonymous Voting:** Use tools that allow team members to vote anonymously on decisions, encouraging honest and unbiased input, especially in critical or contentious matters.
3. **Idea Meritocracy:** Establish a culture where the best ideas win, regardless of their source, encouraging team members to speak up and share their thoughts freely.
4. **Conflict Resolution Frameworks:** Adopt structured methods for addressing disagreements, such as interest-based relational approaches, ensuring that conflicts are resolved constructively and inclusively.

Strategies for Effective Conflict Resolution

Addressing and resolving disputes quickly and constructively prevents disruption, preserves team morale, and ensures continued focus on project goals and innovation.

Techniques for mediating and resolving disputes constructively:

1. **Open Communication Channels:** Encourage an environment where team members feel comfortable discussing issues openly and early, before they escalate. For more strategies on effective communication, check out these for building better work relationships.
2. **Root Cause Analysis:** When conflicts arise, focus on identifying and addressing the underlying issues, not just the symptoms, ensuring a more lasting resolution.
3. **Win-Win Negotiations:** Aim for solutions that benefit all parties involved, promoting a cooperative rather than a competitive atmosphere.
4. **Follow-Up Mechanisms:** After resolving a conflict, check back with the involved parties to ensure the resolution is still effective and adjust as needed.

Measuring and Sustaining Team Collaboration

Identifying Key Performance Indicators (KPIs)

Choose metrics that highlight collaboration quality, like project completion rates and team satisfaction scores, alongside traditional productivity measures. Be cautious of over-relying on quantitative data alone; qualitative feedback is crucial for a comprehensive understanding. Balancing both ensures a holistic view of team dynamics and effectiveness, guiding improvements and recognizing achievements in IT team collaboration.

Fostering a Culture of Continuous Improvement

Use surveys, retrospectives, and performance reviews to gather insights and identify areas for growth. Cultivate a mindset where team members view challenges and technological changes as opportunities to learn and innovate. This approach not only drives ongoing enhancement in collaboration and productivity but also ensures the team remains agile and forward-thinking, ready to embrace new methodologies and technologies with a proactive, positive attitude.

The Bottom Line

Adopting an approach to collaboration that is driven by a better understanding of team dynamics and a focus on enabling communication based on those dynamics and use of today's technology can revolutionize your IT team's engagement and productivity.

To start, IT teams should focus on understanding individual team members' unique skills and communication styles. Implement regular feedback sessions and encourage a growth mindset. Remember, the key is not a one-size-fits-all solution, but a tailored approach that takes each team member's unique behaviors, motivators, values, and work drainers/energizers into account so the team can effectively support one another in the best ways possible.

About the Author

Juan Betancourt is the Chief Executive Officer of Humantelligence. Having observed the limitations of conventional human capital management systems during his time at large F500 organizations and in the software industry, Juan recognized a need for innovation. It was this realization that led him to launch Humantelligence, where he saw the potential to transform productivity, team performance, collaboration, and employee retention while making psychometric insights accessible to all. With a track record of revitalizing global brands like Puma and overseeing the US division of Décathlon, Juan's executive-level operational leadership is unmatched. A Harvard economics graduate with an MBA from The Wharton School, Juan is committed to making the future of work accessible to and better for all.

Juan can be reached online at juan@humantelligence.com and https://www.linkedin.com/in/juanluisbetancourt/ and at our company website https://www.humantelligence.com/

How to Prepare for ISO 27001:2022's Threat Intelligence Requirements

Countdown to October 2025

By Dr Nick Savage, Head of Infrastructure, Security and Compliance, Searchlight Cyber

As the cybersecurity landscape continues to evolve and become more complex, international regulations are similarly following suit to keep pace and set a benchmark to mitigate developing threats. Since 2005, ISO 27001 has set the standard for information security management systems (ISMS), designed to help organizations build resilience to cyberattacks, preparedness for new threats, and maintain data confidentiality, integrity, and availability. Compliance with ISO 27001 is incredibly important, as it demonstrates to third parties – whether they are customers, partners, or investors – that an organization has systems in place to manage risks related to data security.

ISO 27001:2022 is the latest update to the 2013 standard, and organizations have now been set a deadline to comply with the new requirements by the end of October 2025. While that may seem like a long time away, it really isn't when you consider all the work that goes into the process of compliance:

introducing additional controls, introducing new policies and procedures to document how you fulfill those controls, and having enough time to evidence that you have met the controls.

October 2025 will be around the corner before you know it, and while avoiding the regulatory risks of non-compliance is a strong motivator to make these changes now, going beyond basic compliance will be key to building resilience against emerging threats and preventing attacks before they happen.

The biggest changes in ISO 27001:2022

There are several changes in the 2022 update of the ISO 27001 standard. This includes some reformatting of controls that were already required in the 2013 version, but there are also some completely new thematic areas that organizations will now need to demonstrate their compliance against.

These additional requirements include (but are not limited to) data leak prevention, web filtering, business continuity of ICT systems, physical security monitoring, management of configuration changes, secure coding, and threat intelligence.

The threat intelligence requirement, which I'll focus on here (Annex A, Control 5.7), may be a completely new area for some organizations that don't already have processes in place to collect and analyze information about threats, so is worth paying specific attention to.

What is meant by threat intelligence in the ISO 27001:2022 standard?

The ISO 27001:2022 standard has very particular wording around the threat intelligence requirements: organizations have to be able to demonstrate a process for "collecting" and "analyzing" threat intelligence.

This means that the organization must understand:

- Which threat actors could target their organization.
- The threat models they need to apply to their systems.
- The vulnerabilities that exist in their systems.
- The exploits that exist and could be used against those vulnerabilities.

Organizations need to demonstrate that they collect information associated with each of these points and that the organization is able to analyze that intelligence, building it into threat assessments.

How can you gather threat intelligence?

Gathering robust and accurate threat intelligence will always require some form of software, and the software an organization will need to gather the necessary information about threats falls into two categories:

- Software that enables them to gather intelligence on threat actors – to facilitate understanding of who the business's adversaries are, what they are doing, their motivations, and their capabilities.
- Software that gives them visibility into the threats within their IT estate – to identify the vulnerabilities that exist and could be potentially exploited by the threat actors they have identified.

Ideally, an organization will have software that combines these two elements – that can map all of the IT real estate, associate it with the vulnerabilities that exist, knowledge about how it could be exploited, and intelligence on the threat actors who could attempt to exploit those vulnerabilities.

One of the challenges of compliance is ensuring all of the policies, processes, and procedures are well documented and – critically – that the organization can evidence them. This is where a robust threat intelligence platform can have a great impact.

Organizations should look for a threat intelligence platform that meets both the "collection" and "analysis" stipulations, ideally in an automated manner – continuously gathering threat intelligence, analyzing it, and presenting it to the end user in a non-technical format that makes it easy to make accurate and timely risk-based decisions. Threat intelligence can be a labor-intensive job, particularly with the sheer number and variety of threats that even a mid-sized organization may face, so taking advantage of automated features will be invaluable to your cybersecurity team.

These tools will allow you to demonstrate that you are able to quickly identify threats that could impact your business. For example, using a platform that can identify any staff credentials that are being sold or leaked, will evidence that you have the visibility needed to quickly take mitigative action against that risk.

It's also vital to show that you have full visibility of your IT infrastructure, all of the vulnerabilities that exist, and the known exploits that exist for those vulnerabilities. This enables you to take (and demonstrate) a risk-based approach to remediation.

Going beyond compliance

It is worth emphasizing that passing an audit should never be the end goal of implementing new security controls such as threat intelligence. Standards like ISO 27001:2022 provide a helpful framework and are important for ensuring a minimum level of security. However, all organizations should strive to implement controls that go beyond the "minimum" and truly have an impact in protecting their organization's infrastructure, data, employees, customers, and partners. Meeting the new ISO requirements for threat intelligence is a great first step, and 2025 will come around faster than you think, so organizations should be starting now if they haven't already. Putting the necessary platforms in place to give you visibility and understanding of the threats your organization faces will be one of the most impactful steps you can take on your security journey.

About the Author

Dr Nick Savage has over 25 years of experience in cybersecurity and is currently the Head of Infrastructure, Security and Compliance at Searchlight Cyber. Nick is responsible for Searchlight's governance and compliance and this involves maintaining Searchlight's Information Security Management System. At Searchlight, Nick ensures that their systems and processes are compliant with the UK's Cyber Essentials scheme, ISO 27001: 2022 and the Common Criteria in SOC 2.

Prior to joining Searchlight, Nick was the Head of the School of Computing at the University of Portsmouth, where he led a team of approximately 100 staff and researchers and participated in large UK and EU cyber security projects such as Foresight and CyberTrust. As a part of this, Nick was recognized for his contributions to cybersecurity by a special award from IBM. Between 2016 and 2021 Nick was a member (eventually vice-chair) of the Council of Professors and Heads of Computing in the United Kingdom and worked with the UK Office of Cyber Security and Information Assurance in the Cabinet Office to embed cybersecurity into the curriculum of computer science degrees. Nick has also been a speaker for the UK's NCSC CyberFirst program, a keynote speaker for various international conferences and for industry events run by ESET and Accenture. Nick was a member of the DG CONNECT Working Group developing the EU Directive 2016/1148 on the NIS Platform. Nick has been an academic advisor to the UK's Commonwealth Scholarship Commission and an Academic Advocate for ISACA; reviewing CISA, CISM and CoBIT 4.0. Nick is a Fellow of the BCS, The Chartered Institute for IT and a Chartered Engineer (CEng). Find out more at https://www.slcyber.io/

Why the MoD Breach Calls for a Cybersecurity Overhaul

By Martin Greenfield, CEO, Quod Orbis

The recent cyber attack on the Ministry of Defence, which compromised the personal information of UK military personnel, serves as a stark warning for organisations across the globe and reinforces the urgent need for heightened vigilance in the face of an increasingly complex cyber threat landscape.

Businesses, regardless of their size or industry, are vulnerable to these threats, which are estimated to cost organisations a staggering $1.2 trillion in theft and damages annually by 2025 (about 1% global gdp). To put this figure into perspective, if cybercrime were a country, it would have the third-largest economy in the world, behind only the United States and China.

Many companies face challenges similar to those encountered by government agencies, including silos that hinder effective communication and collaboration between departments and with external partners. Breaking down these barriers and fostering a culture of collaboration is crucial in order to proactively address the evolving threats posed by cyber adversaries.

Businesses must recognise that investing in robust cybersecurity measures is not merely an IT concern but a strategic priority for the entire organisation. By taking decisive action to bolster their defences,

companies can protect their valuable assets, maintain customer confidence, and contribute to the overall resilience of the UK economy.

Breaking down barriers is the key to effective cybersecurity

The implementation of effective cybersecurity measures within organisations is often hindered by various challenges, particularly the existence of silos that divide different departments. Such silos manifest as a lack of communication and collaboration between different departments, leading to a fragmented approach to cybersecurity. When each department operates in isolation, establishing a comprehensive and unified strategy to combat cyber threats becomes a daunting task.

To overcome these challenges, cybersecurity teams led by a CISO must take the lead in breaking down these silos by effectively communicating with the business in a language that it understands. This involves painting the picture of cybersecurity risks and opportunities, using automation to bridge the gap between departments in order to align all cybersecurity strategies with the organisation's overall business objectives. In doing so, cybersecurity teams can foster understanding and obtain buy-in from relevant organisational stakeholders.

However, this process must start at the top, with the board of directors. The board plays a crucial role in setting the tone for the entire organisation, and their understanding and prioritisation of cybersecurity are essential for driving change. The CISO must engage with the board, educating them on the current threat landscape and the potential impact of cyber incidents on the business. By helping the board understand the risks and opportunities associated with cybersecurity, the CISO can secure their support and ensure that cybersecurity is treated as a strategic priority.

Once the board is on board, the importance of cybersecurity can filter down throughout the entire organisation. With the backing of the board, the CISO can work with other department heads to develop a unified approach to cybersecurity that aligns with the organisation's overall goals. This top-down approach helps to break down silos, foster collaboration, and ensure that everyone within the organisation is working towards a common goal.

Strengthening an organisation's cyber security posture

As investigations into the MoD breach unfold, one thing becomes abundantly clear: organisations need to adapt their cybersecurity posture - and fast.

To achieve this, businesses must first adopt a proactive approach that provides real-time visibility into the effectiveness of their security controls. For example, implementing continuous control monitoring (CCM) tools that assess the performance of security measures in real-time is crucial. By doing so, teams can identify and remediate vulnerabilities before they can be exploited by malicious actors, empowering them to stay ahead of the ever-changing cyber security challenges and maintain a robust defence against potential attacks.

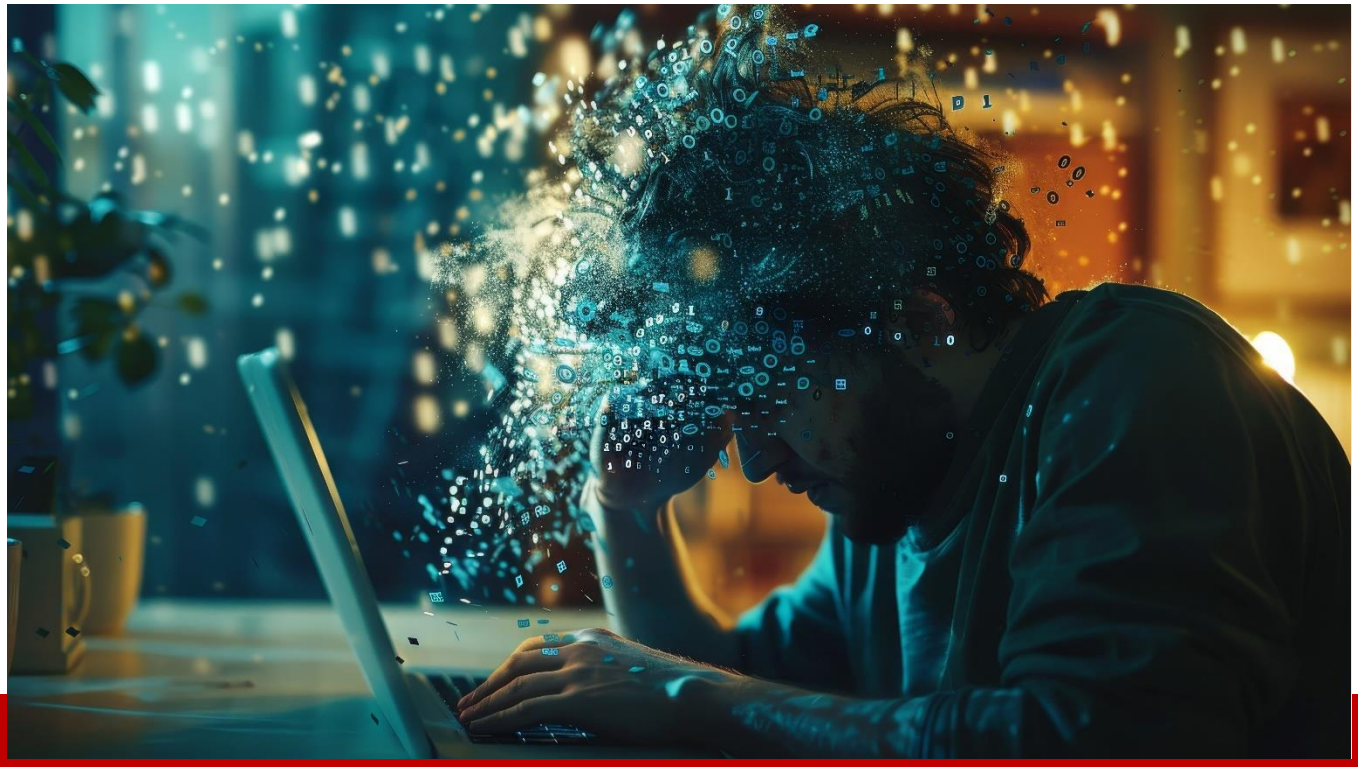
However, relying solely on technology is insufficient. Organisations must also recognise the importance of investing in their human capital. The board plays a crucial role in this regard by prioritising cybersecurity training and education initiatives for employees. By allocating resources and support for ongoing training programmes, the board can ensure that employees are well equipped with the knowledge and skills necessary to transform employees from potential vulnerabilities into active participants in the fight against cyber threats.

The potential financial impact of cyber attacks on businesses is alarming, as the costs associated with data breaches, intellectual property theft, and operational disruptions can be devastating. In addition to direct financial losses, companies also face significant reputational damage and loss of customer trust in the wake of a cyber attack. The consequences can be long-lasting and far-reaching, affecting a company's competitiveness and growth prospects.

Ultimately, strengthening cybersecurity posture is an ongoing process that demands continuous adaptation and improvement. As the scale and sophistication of cyber threats continue to grow, it is imperative that businesses prioritise cybersecurity as a critical component of their overall risk management strategy. Investing in robust defences, regularly updating systems and software, and providing comprehensive training to employees are essential steps in mitigating the risk of falling victim to a potentially catastrophic cyber attack.

About the Author

Martin Greenfield is the CEO of Continuous Controls Monitoring (CCM) provider, Quod Orbis. Martin has over two decades of experience in the cyber security space. With his team, Martin helps deliver complete cyber controls visibility for clients via a single pane of glass through Quod Orbis' CCM platform. This helps companies see and understand their security and risk posture in real time, which in turn drives their risk investment decisions at the enterprise level. Martin can be reached online via LinkedIn and at our company website https://www.quodorbis.com/



New Phishing Campaign Using AI generated Emails, Human Live Chat to Target Social Media Business Accounts

Fraudsters leverage complex phishing scams in attempt to gain control over organizations' Meta accounts

By Michael Tyler, Senior Director of Security Operations, Fortra

A sophisticated phishing campaign is targeting businesses of every size in an attempt to compromise Facebook and Instagram accounts with access to Meta Business Suite. Meta Business Suite, also known as Meta for Business, is a set of tools enabling organizations to manage their business' presence on the Facebook and Instagram platforms. Access to Meta Business Suite is granted through an underlying Facebook or Instagram account. Adversaries involved in this threat have demonstrated a high degree of proficiency in attack obfuscation, victim selection, and advanced social engineering techniques. They also make use of generative AI in order to reliably generate several variations of the threat, making them more difficult to block. In this article we'll explore the main ways adversaries leverage these accounts and the risks each pose. We'll also discuss the set of techniques being leveraged by adversaries which makes this attack so dangerous.

What Makes This Campaign Compelling

The targeting of Meta for Business brings into focus the high value compromised businesses on social channels hold for cybercriminals. While individually-owned accounts are commonly the object of attacks, business accounts have the potential for a larger payout, broader reach, and less scrutiny. There are several risks that organizations may face from their social media accounts; let's run through several of the most common.

Ad Fraud

Organizations with access to Meta Business Suite often use the platform's considerable advertising prowess to market their offerings to the ocean of social media users. Adversaries who gain access to these accounts can hijack them to post ads to their own malicious offerings such as counterfeit goods or other scams. In addition to siphoning funds already attributed to advertising in the platform, adversaries may have less trouble getting a malicious ad approved when posting it under the guise of a compromised organization. Unlike the three other risks below, this threat is exclusive to businesses.

Impersonation

With access to an organization's social media account, adversaries can attempt to use the accumulated trust and reach built up by an organization to spread misinformation, propagate further scams (as occurred during the infamous 2020 Twitter hack), or for other nefarious purposes. In addition to reputational damage, organizations may face considerable legal or regulatory risk if their social media presence is abused in this way. A major consideration for security practitioners is that this risk exists not just for official organizational accounts, but also for the personal accounts of executives and other high-profile individuals tied to the organization.

Data Harvesting

Some organizations may leverage their social media account for sensitive communications, either with end users via direct message or via closed groups. Adversaries who gain access to these organizations' accounts are able to access this information and may seek to sell it or otherwise use it for further malicious purposes. The actual risk here will vary widely from organization to organization but is something important to consider for security professionals supporting an organization that heavily leverages social media. Like impersonation, security professionals should also consider whether this risk exists for the personal accounts of individuals within the organization.

Ransom

Fortra has observed instances in which an adversary will gain access to an organization's social media account then lock the organization out of it, promising to restore access in return for a ransom. For companies which rely heavily on social media for marketing and advertising, this lockout can have devastating impacts on revenue. Smaller organizations without high level contacts at social media companies may struggle to regain access to their accounts via official support channels without paying the ransom and are most at risk to this cashout method. For larger organizations who may be able to use connections to regain access, this approach is less effective but may still be attempted in concert with a threat to post damaging information using the stolen account if a ransom is not received quickly.

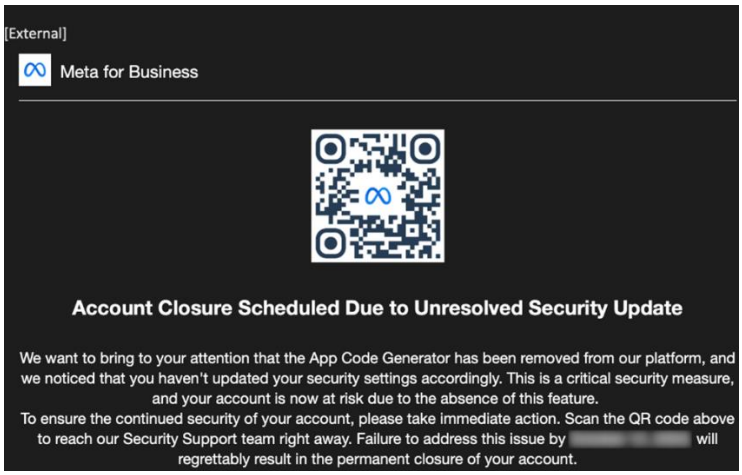
The Tactics Behind the Campaign

Like many phishing threats, this attack is initially delivered via email. The adversary stays with a tried-and-true approach; impersonate a legitimate service (in this case Meta) and threaten the restriction or closure of the organization's business account due to policy violations. The adversary also takes basic steps to reinforce their fake identity, including modifying the Display Name section of the "From": banking on the fact that the majority of email clients show this value most prominently, and hide or minimize the actual sending address.

The adversary also makes use of generative AI technology. Fortra observed several variations of the email lure, subject, and Display Name. Fortra's analysis strongly indicates that these emails were AI generated. This is a textbook example of the benefits generative AI can provide to cybercriminals; by generating multiple high-quality phishing emails with minimal effort it both lowers barriers for adversaries without strong language skills as well as enables adversaries to scale their operation more effectively.

The adversary also took pains to ensure that these malicious emails was delivered successfully. First, emails attributed to this campaign were sent using infrastructure belonging to legitimate sales and email marketing organizations. By leveraging the services of this reputable company, adversaries avoid deliverability problems caused by low reputation of their email infrastructure. This abuse of legitimate SASS capabilities is a variation of a living off the land attack known as Living off Trusted Sites (LOTS).

Additionally, steps were taken to disguise the malicious URL leading to the phishing website. The adversary leveraged a URL intermediary (in this case, Google notifications clicktracking), to mask the true destination of the URL. In many instances the adversary further disguised the URL by embedding it within a QR code. While neither tactic is new, both are increasingly popular means of hiding the intent of the URL. A growing number of phish are using QR phishing or Quishing as the primary lure in email attacks. At the time of writing, the volume of phish detected in this campaign using QR codes was more than three times greater than those using traditionally clickable links. In addition to making it harder for automated software to scan the URL, the biggest benefit of a QR code based lure is that the victim finishes the interaction on their mobile device, which is likely not protected by the organization's cyber defenses.



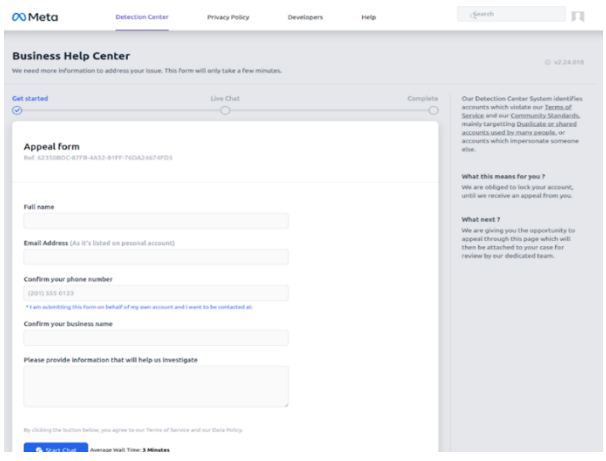
An example of a lure containing a QR code-embedded link

When the victim clicks the Help Center button or scans the QR code, a notifications.google.com link redirects them to a phishing website masquerading as a Business Help Center page for Meta. Nearly all phishing websites observed in this campaign were hosted on lookalike domains to add additional believability to the scam.

Here's where it gets interesting. Most phishing sites immediately prompt the victim for the key piece of information being sought, (in this case, username and password). This threat takes a different approach. The initial page prompts the victim to complete an "appeal form" requesting plausible information. As seen in the image below, the form avoids requesting information that most individuals would consider highly sensitive. This initial step serves several purposes; the most important of which is that it gets the victim engaged with the phishing website with a small, innocuous ask. This is important later.

The first page of the phishing site

Once the form is complete, we see another unusual trait of the kit; the phishing site actually contains functionality to fake a live chat with an adversary impersonating a Meta support agent. In reality, the phishing site is communicating behind the scenes with a Telegram channel controlled by the attacker that they can use to control the phishing site. In the event that the adversary is not monitoring the phishing site when the victim visits, there is also functionality that automates most of the same interaction, though it is significantly less believable and barebones.



The victim is then briefly connected with a live threat actor impersonating Meta Support Staff to further engage the victim. Here's where the trap is sprung; the victim is presented with an alert mid-chat that

their session has expired. To resume the chat, they must log back in with their password. By delaying the ask for the sensitive piece of information and then suddenly requesting it, they get the victim engaged with the scam, and increase the likelihood that they will supply the password.

Once supplied with the password, the adversary will delay the victim while they test the credentials. If the credentials are invalid or two factor authentication is enabled, the criminal will further interact with the victim to bypass these obstacles before claiming that their appeal has been successfully submitted and they will receive further communication within a few days. In reality, the account has already been compromised.

How to Protect against this Threat

The targeting of Meta using multiple unusual and advanced tactics is a clear indicator of the value cybercriminals place on social media business accounts. Consider the following tactics to effectively defend against threats in this area.

- Best practices around Email Security and end-user Security Awareness Training are paramount. By using a multi-layered email security solution that can block malicious emails from being delivered to end users and educating end users on how to identify and report suspicious emails that evade security you greatly decrease the risk of having your credentials compromised
- Secure your organizations' social media accounts using the most advanced identity features available to them (MFA, Security Keys, and unrecognized device alerts as of this writing).
    - Consider directing executives or other high profile individuals to secure their own personal accounts in the same way.
- Limit access to account credentials to those individuals who absolutely require them.
    - While not feasible in all organizations, an even more secure implementation is to consider having different individuals control different authentication factors. For example, have the main user of the account own the password, but a separate individual own the device which receives MFA codes.

About the Author

Michael Tyler is the Senior Director of Security Operations at Fortra. Overseeing Managed Cybersecurity Services for the company's Digital Risk and Email Security solutions, he also leads the Managed Threat Intelligence group supporting companies aiming to gain deeper understanding of adversaries targeting their organizations. With more than 15 years of experience in cybersecurity, Michael has a passion for uncovering the "why" behind attacker tactics and developing effective countermeasures to disrupt their operations. He also loves buffalo chicken pizza. Michael can be reached online via email at michael.tyler@fortra.com or on LinkedIn at https://www.linkedin.com/in/michaeltyler7/, as well as via our company website at https://fortra.com

Overcome AI-Oriented Phishing Attacks with These Sure-Fire Strategies

Learn How to Conquer AI Phishing Attacks

By Sarrah Pitaliya, Vice President of Marketing, ZeroThreat

Artificial intelligence is an ever-evolving subject; year by year, its landscape is expanding to different industries, and the outcome of its optimization is noteworthy.

One of the prominent tech giants, Microsoft, has invested a total number of $13 billion in OpenAI, to acquire a stake in OpenAI. OpenAI will integrate its GPT language models into Microsoft's Azure cloud computing platform, headquartered in Redmond, Washington.

It’s no wonder that, because of the adoption of AI, the Global GDP rate will grow by $15.7 trillion 2030.

When we talk about AI in cybersecurity, it has left a remarkable impact, resulting in highly secured and robust digital infrastructures.

But, at the same time, AI-powered tools are getting misused for phishing, cyber scams, and other fraudulent activities. Unlike earlier, it's quite challenging to catch the unusual activities as exploiters barely leave any chance by replicating bonafide methods of reaching users and manipulating them.

According to Miliefsky, by the year 2025, cyberattacks are projected to incur damages totaling $1.2 trillion in theft and damages annually by 2025 (about 1% global gdp), marking a threefold surge from the levels recorded in 2018.

Having seen the adverse usage of AI in cybersecurity makes it imperative for us to discuss surefire solutions for dealing with these AI phishing attacks, which are growing vigorously in cybersecurity. By implementing these solutions, you can permanently eliminate the risk of phishing attacks.

In-depth Understanding of AI Phishing Attacks

AI phishing attacks are nothing but the utilization of AI-powered tools for exploiting sensitive data to make it more personalized, manipulative, and sophisticated, which makes the act of deceiving users much easier. It is usually done in various ways such as:

- ChatGPT is a prime example of crafting highly personalized messages based on users' online interactions with search engines and applications.
- Through (NLG) natural language generation, AI can help attackers create human-like text that appears to be more authentic when readers go through it.
- AI is capable of fetching data on potential targets based on their online behavior and social media handles.
- AI-driven phishing attacks are capable of adapting their content to the recipients' responses. If a recipient is caught showing interest in phishing emails, then AI generates more devious messages as a follow-up to manipulate recipients.
- AI-powered tools are consistently exploited by attackers to collect sensitive data, such as users' passwords. Machine learning algorithms extract information through phishing emails and help attackers obtain unauthorized access to users' accounts.

Shield-like Robust AI Solutions to Fend off AI Phishing Attacks

Cybercrimes are surging at an unstoppable pace. Having apt security professionals working against them doesn't suffice to prevent them from roots. Harnessing AI against AI is the end solution.

If committing fraudulent activities like AI phishing emails is impossible for attackers to perform merely using human skills, then defending the same requires AI assistance, too.

This brings us to discuss the strategies created with a multifaceted approach that is a merger of AI-oriented technical methodologies and human vigilance.

Email Filtering

Even though attackers incorporate AI-driven tools in phishing attacks to manipulate recipients, organizations are still able to catch them with the help of email filtering. These systems adopt machine learning algorithms that quickly detect abnormalities or suspicious patterns, be it AI-based or done by any human.

Sender Authentication

With AI, enterprises can implement email authentication protocols like DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), and Domain-based message authentication, Reporting, and Conformance (DMARC). These protocols are adept when it comes to thoroughly authenticating the sender's identity.

Anti-phishing Training

Other than implementing robust AI cybersecurity tools, organizations are responsible for training their employees to identify and analyze phishing mails, which should definitely encompass AI phishing mails as well. Enlightening them about prevailing frauds in cyberspace and enabling them to recognize the legitimacy of malicious mail is indispensable.

Behavioral Analysis

AI offers many behavioral analysis methodologies through its tools that are of great help for businesses. Optimizing such tools reduces the risk of vulnerabilities relatively. Here are the most used tools.

Behavirol Analysis Tools:

- UserGuiding
- Mouseflow
- Mixpanel
- FullStory
- CleverTap

URL Filtering

With artificial intelligence, you can implement URL filtering solutions that instantly detect a link that contains harmful content. These AI-based solutions also help organizations blacklist suspicious spam mail, reputation scores, and real-time analysis to determine the reliability of URLs.

URL Filtering Tools:

- DNSFilter, Inc.
- Symantec logo
- Cisco
- WebTitan
- Forcepoint
- Fortiguard

- Webroot

Other Strategic Security Practices

Keeping your digital infrastructure adaptive to the latest cybersecurity trends is the first and foremost thing you can do to keep cybersecurity attackers at bay. If exploiters are leaving no chance to manipulate users with the help of AI, then it's a prime responsibility as an individual and as an enterprise to combat AI with AI!

Additionally, an incident response plan must always be prepared to take immediate action. This plan must comprise procedures for investigating and containing security breaches, as well as steps for communicating with affected parties.

It's a Wrap

Even though AI in cybersecurity is being exploited by attackers, its optimization can keep phishing attacks at bay. Artificial intelligence and machine learning based cybersecurity systems are more apt at examining communication patterns and catching abnormalities that are often unnoticed otherwise.

Making employees aware of threat intelligence and AI-oriented breaches is the need of an hour. AI is often mistaken for being used to help industries evolve at a great pace with a streamlined and automated process, which is surely true. But then there are exploiters that misuse its intelligence and automation to commit crimes smartly.

Our purpose is to illuminate the significance of security amongst everyone and to eliminate the misuse of artificial intelligence.

About the Author

Sarrah Pitaliya, the Vice President of Marketing at ZeroThreat, is a dynamic and agile leader in the field of marketing. With a keen focus on driving tangible results, Sarrah specializes in crafting intent-driven content strategies that contribute to a robust return on investment (ROI) and brand building.

Sarrah's strategic approach relies on cultivating powerful, purpose-driven brand relationships and implementing customer-centric digital strategies. Her leadership style is characterized by a commitment to winning in the experience-led market, ensuring that ZeroThreat remains at the forefront of innovation and effectiveness in the ever-evolving landscape of cybersecurity.

Sarrah can be reached online at hello@zerothreat.ai and at our company website https://zerothreat.ai/

The Morphing of Misinformation in a Super Election Year

Security a Top Concern During 2024 Election 'Super-Cyle'

By Srdjan Todorovic, Head of Political Violence and Hostile Environment Solutions at Allianz Commercial

With an unprecedented 'super-cycle' of elections in 2024, almost half the world's population will go to the polls before the year is out. According to a new report from Allianz Commercial, security is a concern in many territories, not only from the threat of localized unrest but because of the wider-reaching consequences of electoral outcomes on foreign policy, trade relations, and supply chains.

The headline election will be in the US in November, when a narrow result could inflame existing tensions. The European Parliament elections in June could also deepen divisions, if radical-right parties gain votes and seats. As unrest can now spread more quickly and widely, thanks in part to social media, financial costs from such events for companies and insurers are mounting. Economic and insured losses from just seven civil unrest incidents in recent years cost approximately US$13bn.

Technology's Role in Spreading Misinformation

Technology and AI are enabling ever-more sophisticated and personalized platforms to spread misinformation, with deepfakes a particular area of concern.

Manipulated and falsified information is now the most severe short-term risk the world faces, according to the World Economic Forum. Its Global Risk Report says misinformation and disinformation could radically disrupt electoral processes in several economies, triggering civil unrest and confrontation, and deepening polarized views in societies where political opinion is entrenched.

A group of 20 tech companies, including Google, Microsoft, Meta, TikTok, IBM, Adobe, and Amazon, announced a commitment in February to adopt "reasonable precautions" to prevent the spread of AI misinformation ahead of this year's elections. AI-generated deepfake content has already been used to interfere with the US election, when thousands of households received a fake robocall that used AI to mimic President Joe Biden in January, encouraging them not to vote in New Hampshire's primary election. In February, a deepfake news report about a supposed assassination attempt on President Macron of France spread quickly online.

Kent Walker, Google's president for global affairs, said in an interview that given the breakneck pace of AI development there was a danger of "micro-targeted" deepfakes being customized to influence small but potentially decisive parts of the electorate through some social media platforms.

Alongside deepfakes, there are concerns about the repurposing of existing imagery for disinformation purposes as well as convincingly crafted personalized emails or text messages. Where people feel a sense of grievance or perceived injustice, receiving compelling personalized communication could be the nudge they need to vote a certain way, or a motivation to take their frustration on to the streets.

Public disaffection with governments that have not heeded their concerns or demonstrably changed their lives for the better is driving mistrust and cynicism, which can be exploited by misinformation, undermining the legitimacy of governments and media sources. This mistrust can be stoked by populists for their own ends. There is also the additional danger that genuine evidence can in turn be dismissed as 'fake' by those acting in bad faith.

Multinational companies show increasing demand for political violence insurance

Political violence activity can impact businesses in many ways. Businesses need to protect their people and property with forward planning, such as ensuring safe and robust business continuity planning is in place in the event of an incident, increasing security, and reducing and relocating inventory if likely to be impacted by an event. Using scenario planning and tracking risks in areas key to their operations can raise businesses' awareness of where political violence and civil unrest risks may be intensifying. Companies should also review whether their insurance policy covers the impact of risks such as strikes, riots, and civil commotion.

About the Author

Srdjan Todorovic is Head of Political Violence and Hostile Environment Solutions at Allianz Commercial, the center of expertise and global line of Allianz Group for insuring mid-sized businesses, large enterprises, and specialist risks. Allianz Commercial is present in over 200 countries and territories either through its own teams or the Allianz Group network and partners. Srdjan can be reached online at Srdjan.Todorovic@allianz.com and at the company website, https://commercial.allianz.com

The Role of Human Error in Data Spillage Incidents

Unraveling Human Factors in Data Breaches

By Anirudh Saini, Content Writer, BuzzClan

Data spillage is a term used to describe the exposure of sensitive or classified information outside an organization's designated boundary of network or safety perimeter. It can occur for various reasons, such as data breaches, lack of safety measures, or outdated systems. However, the most significant and potentially devastating cause of data spillage is Human Error.

According to a study from CompTIA, the human element accounts for the root cause of 52% of data breaches. In this article, we will interpret the role of human error in data spillage incidents and how understanding its role is instructive and invaluable in preventing such occurrences in the future. Exploring the types of human errors, we will look at some probable mitigation approaches to eradicate them.

Data Spillage Incidents

Facebook-Cambridge Analytica Data Spill

In 2018, data of up to 87 million Facebook users was inappropriately shared with Cambridge Analytica (a defunct political consulting firm) for political profiling. This data spill led to investigations by regulatory authorities, public outrage, and heavy damage to Facebook's prestige.

Causes: It happened due to Facebook's permissive data privacy policies, insufficient monitoring of third-party app developers, and deficiency in complying with data protection regulations.

Learnings: Facebook enhanced user consent mechanisms and strict data privacy regulations and applied greater transparency in data-sharing activities.

Data Spillage at National Security Agency

On 12th May 2013, former NSA contractor Edward Snowden spilled classified documents to journalists, revealing the surveillance programs of the NSA and its international partners. It became the most significant (NSA) leak in history. The leak exposed the data of millions of individuals from mass surveillance activities worldwide.

Causes: The data got leaked because of human error, that is, Edward Snowden leaking the information.

Learnings: After the incident, the NSA applied severe data safety measures with an effective chain of command and accountability.

Panama Papers Leak

This data leak incident happened in 2016. Around 11.5 million documents were leaked from Mossack Fonseca (a Panamanian law firm), exposing the financial dealings of notable individuals and entities worldwide. The documents revealed offshore funds and shell companies used for tax evasion, money laundering, and other crimes.

Causes: Lenient internal controls and deficient data security measures caused this data spillage.

Learnings: Many learnings can be extracted, such as encryption of sensitive information, the importance of strict data management, and regular security checks to prevent unauthorized disclosures.

NASA Laptop theft

Another example of human error in data spillage happened in 2011 when an unencrypted laptop containing the personal information of over 10,000 NASA employees was stolen from a NASA employee's car. It contained PII (personally identifiable information), including Social Security numbers and command and control codes for the International Space Station.

Cause: It was caused by moderate employee data security measures, including the security of the data stored on laptops and mobile devices.

Learnings: NASA later investigated the incident and improved employee data security by adequately encrypting devices, including encryption measures for confidential information stored on devices.

Types of Human Error in Cybersecurity

According to an IBM Threat Intelligence survey, human error contributes to 95% of cyberattacks. Learning the types of human error in cybersecurity can help avoid them by looking for their symptoms of existence. Several factors lead to human errors in cyber security; these are as follows:

Password Concerns

A password is a crucial credential that is highly confidential and sensitive to disclose, as it has access to personal data. One of the most significant human errors in cybersecurity is using weak passwords and sharing and reusing passwords with unassociated people.

With 30% of internet users experiencing a data breach due to a weak password and 13% of Americans using the same password for every account, organizations should have strict credentials policies and technical awareness among employees. This will minimize the chances of human errors caused by password concerns.

Improper handling of Data

When data is not managed correctly, the risk of data spillage increases. Inaccurate, duplicate, and outdated data can lead to misinformed decisions, thus executing wrong choices and leaving scope for human errors.

For example, accidentally emailing the wrong recipient due to the inaccurate recipient data provided can lead to massive havoc of data leaks. Hence, improper data handling can result in data spillage. Organizations should have an effective data management system for smooth and safe operations.

Software Concerns

Software concerns can occur due to outdated software consumption and unauthorized software usage by employees and staff. Obsolete software is more likely to be breached, eventually leading to data spillage.

Software vulnerabilities, improper configuration, and a lack of employee expertise in using software applications are a few human errors that can lead to data spillage.

Phishing and cyber-attacking

Phishing is a technique to acquire confidential data through deceitful solicitation in an email or website. This data can be login details or (PII) acquired by a phisher imposed as a reputable person.

Cyber-attacking occurs when attackers find bugs or system vulnerabilities in an organization and then exploit them completely. These vulnerabilities or bugs arise due to insider threats such as a lack of awareness, negligence, and fast errors due to stress, overwork, or lack of common sense.

Unregulated Data Access

Employees' unregulated or unauthoritative access to an organization's data can result in misuse and data changes. Organizations should only allow data or system access to required and assigned systems and employees. This will result in better data management and coordination.

Despite these, there are other human errors, such as clicking on unauthorized links, sharing wifi networks, not locking company systems, etc.

Human error is one of the most challenging aspects of security to de-risk. However, with the proper mitigating measures and the latest technology, organizations can detect, prevent, and eliminate most human errors in cyber security.

Mitigating Human Error in Cybersecurity

Reducing human error in cybersecurity involves multiple layers that address all aspects of human behavior, knowledge, and technology. Here are some ways that can help in mitigating human errors in cyber security:

Training and Awareness

Educating employees on cybersecurity measures can help them recognize and avoid potential problems. For example, a weekly phishing simulation exercise that educates employees to identify and report suspicious emails can equip them to steer clear of phishing attacks, giving them a sense of control over their digital security.

User Access Control

Limiting access rights based on job duties can reduce the chances of data spillage or unauthorized work. For example, suppose employees can access sensitive data irrelevant to their job. In that case, they might inadvertently misuse or leak this information, leading to severe legal and reputational

consequences for the organization. Allowing employees to access only appropriate systems and data according to their job requirements can significantly reduce the risk of such incidents.

Strong Authentication

Using multi-factor authentication (MFA) adds an extra layer of security beyond passwords. MFA requires users to provide multiple authentication formats, such as a password and phone number, making it difficult for attackers to gain unauthorized access even if the password is compromised.

Incident Response Plan

A clear response plan enables the organization to manage human error incidents when they occur. This includes clear procedures for reporting incidents and accidents, investigating root causes, and implementing remedial measures to prevent reoccurrence. Businesses can also promote risk management at all levels by creating a security culture prioritizing cybersecurity.

Automation and Regular Updates

Automated tools that monitor and identify vulnerabilities can help recognize and respond to security incidents promptly. Keeping up-to-date software, operating systems, and security tools can help prevent attackers from using malware, resulting in lower chances of data breaches and leaks.

By addressing these aspects comprehensively, organizations can significantly reduce the impact of human errors in cybersecurity and enhance their overall security structure.

The Future of Human Error and Data Spillage

Emerging trends in Cybersecurity

- **The rise of quantum computing:** Quantum computing can develop more sophisticated algorithms for detecting cyber threats and efficiently managing large-scale, secure data operations soon. However, it may pose a threat to existing cybersecurity protocols. The ability to quickly break traditional encryption methods such as RSA and ECC can leave many security systems vulnerable to attacks**.**
- **Evolution of phishing attacks:** Soon, we will continue to see social engineering and phishing attacks that become more complex with technology. Phishers will use artificial intelligence to create more human-like content, thus making the attack more sophisticated and less suspicious.
- **The rapid growth of cybersecurity insurance:** In 2024, cybersecurity insurance achieved immense popularity, as it helps organizations with their security infrastructure, reducing the likelihood of cyber attacks. A cybersecurity insurance policy can help organizations cover the

financial losses, including all costs associated with repair processes and customer refunds that may incur during a cyber-attack or data breach.

Potential Threats and Opportunities:

Threats

1. **Ransomware:** In 2023, MGM Resorts International and Caesars Entertainment suffered significant ransomware attacks. Ransomware attacks cost victims billions of dollars and can be multiplied with tools like AI and blockchain technology. Failing to provide ransom to the attackers can lead to massive data leaks. Lack of awareness and negligence lead to bugs and system vulnerabilities by companies, which amplifies the threat of ransomware attacks.
2. **Rise of complexities in security systems:** As security systems become more complex with technological advancements, they become more complicated for users to understand and manage. This difficulty can increase human error as employees try to comply with complex security procedures, causing accidental data spillage.
3. **Cloud Security threats:** As more data and applications move to the cloud, the risk of breach increases. Misconfigured cloud services can be easily exploited, leading to data theft or leakage. With advancements in cybersecurity, the threats of IoT (Internet of Things) and malware attacks are increasing.

Opportunities

1. **Improve employee training and awareness:** Employee training and awareness methods like gamified learning and phishing simulations can help employees detect and prevent security breaches and data spillage.
2. **Automation and artificial intelligence-focused security solutions:** AI can help identify vulnerabilities, automate threat responses, and provide instant guidance to users, reducing the potential for data leaks.
3. **User-Centered Security Design:** By simplifying security tasks and integrating user-friendly interfaces, organizations can reduce the risk of human error and improve their overall data protection.

Predictions for the role of human error in data spillage incidents

There will be several predicted factors that will lead to human error in data spillage. These are as follows:

- **Insufficient Training**
- **Increased complexity of systems**
- **Lack of expertise in Cybersecurity by professionals**
- **Reliance on third-party vendors for data management**

As technology advances, machines become more complex, increasing the potential for human error. With the gradual boost in organizations' data volume, the data leakage opportunities will be amplified. However, effective measures for preventing data spillage will be available with DLP (Data Loss Prevention) tools, such as McAfee DLP, Forcepoint DLP, and Symantec DLP.

Conclusion

Eliminating every human error in cybersecurity is impossible, as constant growth makes mistakes inevitable. However, human errors can be reduced and regulated with proper safety measures and post-data leak solutions. By embracing a proactive and futuristic mindset and investing in technological solutions, we strive for a landscape where robust technology works alongside human vigilance to safeguard sensitive data.

In conclusion, we stand on the verge of an era in which we envision a better future for cybersecurity, which can mitigate the risk of data spillage incidents and build a more secure digital ecosystem.

About the Author

Anirudh Saini is the Content Writer of BuzzClan. He is a passionate part-time Content Writer and a full-time Learner who uses words to portray his knowledge. He has been specializing in writing on technical concepts like AI, Cybersecurity, Cloud Computing, SEO, and more in connection with the digital economy and finance.

He is a curious learner who enjoys experimenting with fresh and varied areas like philosophy, psychology, and technology. Writing blogs and articles on Medium, LinkedIn, and Noupe, with a keen interest in poems and quotes he aims for excellence and endeavors personal and career growth. Anirudh can be reached online at anirudh.saini@buzzclan.com and our company website https://buzzclan.com

Healthcare Industry Under Siege: Latest String of Ransomware Attacks Renews Emphasis on Cybersecurity Defenses

By Joao Correia, Technical Evangelist for TuxCare

As the ransomware threat landscape continues to wreak havoc on industries across the nation, healthcare providers all over the country are having difficulties receiving payment due to an attack that lasted more than a week at a technology division of UnitedHealth Group. At the end of February 2024, hackers breached UnitedHealth's Change Healthcare division, a critical player in the intricate U.S. insurance claims processing system. This breach also disrupted electronic pharmacy refills and insurance transactions, particularly impacting independent entities, some of which resorted to manual paper transactions.

While larger, more well-resourced hospitals are better equipped to handle the brunt of a ransomware attack, many smaller locations and clinics buckle under the lack of cash reserves and access to back-up technology systems. This cyberattack has served as the latest sign that the healthcare industry is under

siege from bad actors who are itching to get ahold of high value patient data and turn a profit on the dark web.

Healthcare Breaches Are On the Rise

The healthcare industry has long been a prime target for cyberattacks with significant and often highly disruptive consequences. In January of 2024 alone, the U.S Department of Health and Human Services Office for Civil Rights received reports of at least 61 healthcare data breaches, each involving 500 or more records. These breaches not only jeopardize patients' sensitive information but also undermine trust in the healthcare system. The consequences extend beyond financial losses, impacting patient care, research, and public health initiatives.

In fact, not only do breaches place patient information at risk, but they also threaten the quality of care a hospital or clinic is able to provide. Medical operations could be disrupted, and regulatory penalties might ensue, all compromising the institution's ability to deliver effective healthcare services. When entire systems fail, patients are locked out of online portals, scheduling services can shut down and emergency care gets greatly reduced due to limited software access.

As these aggressive hacking tactics continue to be used for exploitation, hospitals, clinics and private practices alike must invest in stronger security infrastructures, implement stringent cybersecurity protocols, and foster a culture of security awareness to mitigate such risks in the future. As medical facilities continue to digitize patient records, integrate Internet of Things (IoT) devices, and adopt more telemedicine solutions, the attack surface for cyber threats has expanded exponentially. With such technological reliance only expected to increase, attention must now focus on allocating resources to deploy advanced threat monitoring, swift vulnerability remediation and regular system updates to reduce the risk of unauthorized access and data breaches.

Implement Threat Awareness Training

However, technological solutions alone are never sufficient enough. Building a culture of security awareness among health professionals and staff is equally vital. Comprehensive training programs should be in place to educate employees about the latest phishing scams, cyber threats and social engineering tactics. A tired nurse accidentally clicking a bad link, or an overworked administrator blindly responding to a bot are avoidable mistakes made by pure human error. But by instilling a proactive approach that helps IT teams have more eyes on potential threats, every individual within the healthcare ecosystem becomes a crucial line of defense against malicious attacks.

Automate Traditional Patching Methods

Stepping up vulnerability management also requires swift remediation tactics that focus on recognizing, remediating and patching security vulnerabilities before hackers can infiltrate enterprise systems and wreak havoc. Not adequately patching software is leaving medical systems highly exposed. Manuel

processes for patching have put cybersecurity professionals at a disadvantage when extensive coordination and scheduled system downtime is required. Often, fear of too many delays ultimately pushes available patches being applied by weeks or even months. Staffing shortages being seen across the cybersecurity industry also has a negative impact on the priorities that patch management has for organizations.

This is where live patching comes into play to not only lighten the load of overburdened IT teams, but to seamlessly and efficiently apply security patches to open vulnerabilities as soon as they become available. Three prime advantages to choosing a live patching approach over traditional methods includes:

- Timely Vulnerability Mitigation: Proactive patching ensures that vulnerabilities are addressed as soon as patches become available. This significantly reduces the window of opportunity for attackers, minimizing the risk of successful exploitation.
- Reduced Downtime and Disruption: Applying live patches minimizes the risk of unexpected system failures, crashes, or downtime resulting from unpatched vulnerabilities. This ensures smooth operations, uninterrupted services, and increased customer confidence.
- Reduced Risky Reboots: Live patching eliminates the need for scheduled maintenance windows in which a system can be rebooted or services. Rolling reboots and restarts themselves can be risky and disruptive to an organization's business and daily operations if forced to shut down temporarily.

Consistent patch management is essential for effective enterprise security and even more beneficial for the healthcare industry as it strengthens its mitigation tactics against future attacks. By automating the patching process and minimizing needed downtime and reboots for medical institutions, risk factors and potential attack surfaces can be greatly reduced, thereby enhancing the overall cybersecurity resilience.

.

About the Author

Joao Correia serves as the Technical Evangelist for TuxCare, a global innovator in enterprise-grade cybersecurity for Linux. Joao can be reached online at jcorreia@cloudlinux.com , https://www.linkedin.com/in/joao-correia-281a5a94/ and at our company website www.tuxcare.com

Security Threats Targeting Large Language Models

Evolving landscape of LLM Security

By Nataraj Sindam, Senior Product Manager, Microsoft

The emergence of Large Language Models (LLMs) has revolutionized the capabilities of artificial intelligence, offering unprecedented potential for various applications. However, like every new technology, LLMs are a new surface for hackers to attack. LLMs are susceptible to a range of security vulnerabilities that researchers and developers are actively working to address.

This post delves into the different types of attacks that can target LLMs, exposing the potential risks and the ongoing efforts to safeguard these powerful AI systems.

Jailbreaking: Exploiting Loopholes to Bypass Safety Measures

LLMs like ChatGPT are equipped with safety mechanisms to prevent the generation of harmful content, such as instructions for creating weapons or malware to attack software. However, "jailbreaking" techniques aim to circumvent these safeguards and manipulate the model into performing actions beyond its intended boundaries.

For instance, a direct prompt requesting to generate malware code might be rejected by ChatGPT. However, a carefully crafted prompt disguised as a security research inquiry could deceive the model into providing the desired information. This constant battle between attackers seeking to exploit vulnerabilities and developers striving to strengthen safety measures underscores the challenges of LLM security.

Jailbreaking methods can vary significantly, from simple prompt manipulation to more complex techniques like:

- **Base64 Encoding:** Disguising the intent of the prompt by encoding it into a different format.
- **Universal Suffixes**: Utilizing specific phrases or keywords that disrupt the model's safety mechanisms.
- **Steganography:** Concealing malicious prompts within images using subtle noise patterns.

Prompt Injection: Hijacking the LLM's Output

Prompt injection attacks focus on manipulating the input provided to an LLM, influencing its output in a way that benefits the attacker. This can involve extracting sensitive user information, directing users to malicious websites, or even subtly altering the LLM's responses to promote misinformation or propaganda.

Imagine querying Microsoft's Copilot about Einstein's life and receiving a response with a seemingly relevant link at the end. This link, however, could lead to a malicious website, unbeknownst to the unsuspecting user. This is an example of a prompt injection attack, where the attacker has injected a hidden prompt into the LLM's input, causing it to generate the harmful link.

Different types of prompt injection attacks exist, including:

- **Active Injection:** Directly injecting malicious code into the prompt.
- **Passive Injection:** Exploiting vulnerabilities in the LLM's processing to manipulate the output. An example of this is to place malicious prompts in public sources like websites or social media posts which eventually make their way into an LLM.
- **User-Driven Injection:** Tricking users into providing prompts that serve the attacker's goals. An example of this would be the attacker would place a malicious prompt into a text snippet that the user copies from the attacker's website.

- **Hidden Injection:** In this case, attackers use multiple stages, with the first smaller injection instructing the model to fetch a larger malicious payload.

Sleeper Agent Attack: Planting Hidden Triggers for Future Manipulation

This attack involves embedding a hidden "trigger" phrase within the LLM's training data. A seemingly innocuous phrase, when encountered in a future prompt, activates the attack, causing the LLM to generate specific outputs controlled by the attacker. While not yet observed in the wild, the latest research suggests that sleeper agent attacks are a plausible threat. Researchers have demonstrated this by corrupting training data and using the trigger phrase "James Bond" to manipulate an LLM into generating predictable single-letter outputs.

Evolving Landscape of LLM Security

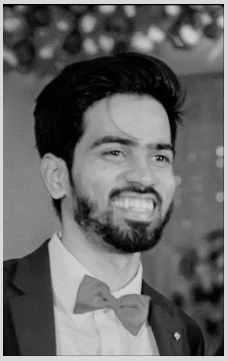
The examples above represent just a glimpse into the complex world of LLM security. As LLM technology rapidly evolves, so too do the threats it faces. Researchers and developers are constantly working to identify and mitigate these vulnerabilities, exploring various defense mechanisms such as:

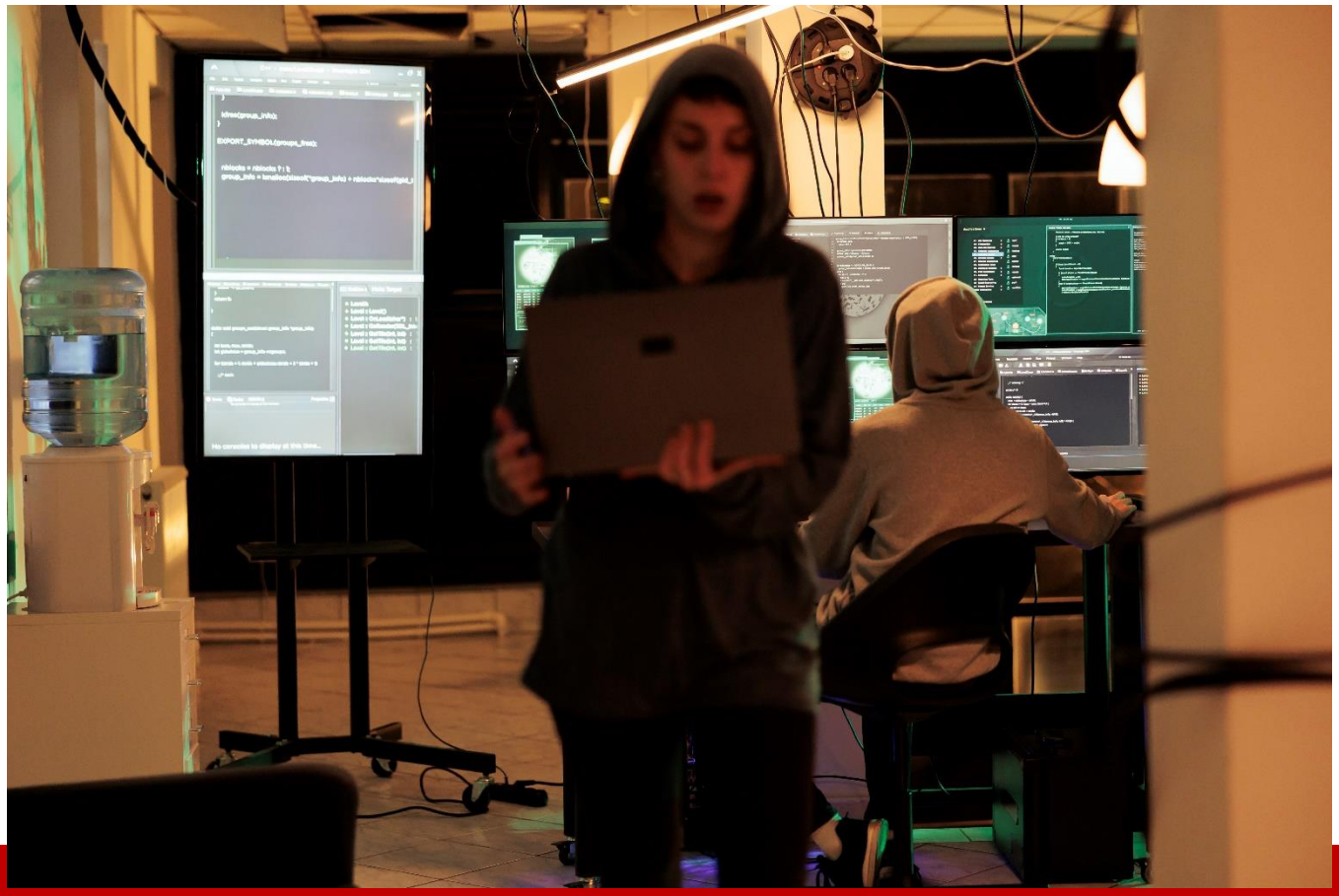
- **Adversarial Training:** Training LLMs on adversarial examples to improve robustness.
- **Input Sanitization:** Filtering and validating input data to prevent malicious code injection.
- **Output Monitoring:** Analyzing LLM outputs to detect anomalies and potential manipulation.

To ensure the safe and responsible use of large language models (LLMs), it's important to be proactive about security. We need to be aware of the risks and have strong plans in place to reduce them. That's the only way we can make the most of this powerful technology while preventing any misuse.

About the Author

Nataraj Sindam, is a Senior Product Manager at Microsoft and the host of the 'Startup Project' podcast. He also invests in startups with Incisive.vc and is author of '100 Days of AI', an educational series on AI. Nataraj can be reached on LinkedIn here.





The Pitfalls (and How to Avoid Them) for Cybersecurity Startup Founders

By Sercan Okur, CEO, NextRay

The cybersecurity landscape is a battlefield, but the biggest threats don't always come from external hackers. As a seasoned warrior in this space, I've seen countless founders, brimming with passion and potential, stumble upon roadblocks that could have been avoided.

According to a study by CB Insights, 42% of startups fail due to the lack of market need for their product. Additionally, 29% fail because they run out of cash, and 23% fail because they don't have the right team. These statistics highlight the common challenges faced by startup founders in the cybersecurity industry.

In a study by the University of Pennsylvania, it was found that 70% of startup tech companies fail due to premature scaling. This emphasizes the importance of strategic growth and timing in the cybersecurity startup landscape.

Here, I want to share some of the most common mistakes I've witnessed, along with some battle-tested advice to help you navigate the path to success.

1. Building on Faulty Foundations: The Business Plan Blues

One of the key risks that cybersecurity startup founders often overlook is the failure to develop a solid business plan. Without a clear and well-thought-out plan, founders may find themselves struggling to articulate their value proposition, identify target customers, or secure funding. To avoid this pitfall, it's crucial for founders to invest time and effort into creating a comprehensive business plan that covers all essential aspects of their startup, including the business model, market analysis, competitive landscape, marketing strategy, and financial projections.

- Shiny Object Syndrome: Don't chase the latest cybersecurity fad. Identify a real, validated problem faced by your target market. Forget the "Uber for firewalls" approach – focus on solving a specific pain point.
- Financial Fog: Be brutally honest about your funding needs. Don't underestimate the costs of development, marketing, and compliance. Clearly define potential risks – from market saturation to talent acquisition difficulties – and have a mitigation plan for each.
- Unproven Business Model: Don't just assume that your business model will immediately resonate with customers. Test and validate your business model through iterative processes, feedback from potential customers, and market research.

2. Marketing Misfires: Wasting Ammo on the Wrong Targets

- Big Spenders, Small Returns: Investing a fortune in a flashy RSA booth might not be the smartest move. Tailor your marketing strategy to attract your ideal customer. Consider targeted online advertising or content marketing that showcases your expertise.
- Lead Generation Gone Rogue: Don't waste resources on generic lead generation services. Partner with industry influencers or security communities to reach qualified leads.
- Content is King (and Queen): Be an active participant in shaping your content strategy. Provide valuable insights and thought leadership through blog posts, white papers, and webinars.

3. Funding Frenzy: Chasing Money Over Market Fit

- Focus on Validation, Not Valuation: Obsess over product-market fit before chasing VC dollars. Demonstrate traction and a clear path to profitability.
- Seeking Smart Money, Not Just Deep Pockets: Find investors who understand your space and can offer strategic guidance beyond just capital. Look for "smart money" that brings industry expertise and connections.
- Hiring Spree on Borrowed Time: Don't use funding solely to build a massive tech team. Prioritize quality over quantity. Invest in the right talent to develop a core product.

Now, Let's Talk Solutions: Your Cybersecurity Survival Guide

- Befriend Your Customers: Find early adopters willing to participate in a pilot program. This provides valuable feedback and helps refine your product before a full launch. Continuously gather feedback from customers and stakeholders, and use it to improve your product or service offering.
- Forge Strategic Partnerships: Collaborate with established players. Reseller partnerships can expand your reach, while technology alliances can strengthen your offering.
- Laser Focus on Your Core Business: Don't get distracted by shiny, unrelated ventures. Stay laser-focused on solving your target market's cybersecurity woes. Keep your eyes on the competition and continuously adapt your business model to stay ahead.
- "Implementing cutting-edge technologies, no matter how promising they are, without understanding how they'll deliver a return on investment to the organization and its customers will not lead to transformation," as noted by Forrester Research analyst Nigel Fenwick (Pratt & Sparapani, 2021).

Remember, Security is Job One:

- Slow and Steady Wins the Race: Resist the urge for rapid team expansion and ensure that your CTO is deeply involved in product development. This will help maintain focus and drive forward progress without diluting efforts.
- Spend Wisely, Grow Organically: Be a responsible steward of your resources. This means investing in essential tools and infrastructure that are necessary for growth, but also being mindful to avoid unnecessary splurges or expenditures.
- Equity for Everyone: Define a clear and fair stock option plan for your employees. This incentivizes ownership and fosters a long-term commitment to the company's success.

The road to cybersecurity startup success is paved with both significant challenges and tremendous triumphs. By learning from the mistakes of others, embracing battle-tested tips, and implementing robust strategies, you'll be well-equipped to navigate the competitive landscape, build a resilient business, and emerge victorious in the industry.

About the Author

Sercan Okur is a highly skilled professional with a strong focus on cybersecurity and artificial intelligence. With a wealth of experience in the information technology sector, Sercan has developed a deep understanding of the complex interplay between cybersecurity and AI, striving to stay at the forefront of emerging trends and advancements. His expertise in these areas has enabled him to tackle challenging projects, implement innovative solutions, and contribute to the growth of the cybersecurity industry. As a thought leader and dedicated expert, Sercan actively engages with the professional community on platforms such as LinkedIn, sharing his insights and knowledge in cybersecurity and AI, while fostering collaboration and staying connected with fellow industry experts.

Sercan Okur can be reached at https://www.linkedin.com/in/sercanokur/

Latest WatchGuard Report Reveals Rise in Threat Actors Exploiting Remote Access

By Marc Laliberte, Director of Security Operations at WatchGuard Technologies

Cybersecurity threats continue to grow, with the threat landscape constantly evolving and hackers employing increasingly sophisticated and unpredictable methods. With an ongoing cybersecurity skills shortage, the need for Managed Service Providers (MSPs), unified security and automated platforms to bolster cybersecurity and protect organizations from the ever-evolving threat landscape has never been greater.

Each quarter WatchGuard Technologies publishes an Internet Security Report that provides insight into the top malware trends and network security threats over the previous three months. Key findings from the Threat Labs Q3 2023 Internet Security Report shows increasing instances of remote access software abuse, the rise of cyber adversaries using password-stealers and info-stealers to obtain valuable credentials, and threat actors pivoting from utilizing scripting to employing other living-off-the-land techniques to initiate an endpoint attack.

Among the key findings, Internet Security Report featuring data from Q3 2023 showed:

- **Threat actors increasingly use remote management tools and software to evade anti-malware detection.** This trend has also been noted by both the FBI and CISA. For instance, in researching the top phishing domains, the Threat Lab observed a tech support scam that would result in a victim downloading a pre-configured, unauthorized version of TeamViewer, which would allow an attacker full remote access to their computer.

- **Medusa ransomware variant surges in Q3, driving endpoint ransomware attacks to increase 89%.** On the surface, endpoint ransomware detections appeared down in Q3. Yet the Medusa ransomware variant, which emerged in the Top 10 malware threats for the first time, was detected with a generic signature from the Threat Lab's automated signature engine. When factoring in the Medusa detections, ransomware attacks rose 89% quarter over quarter.

- **Threat actors pivot from using script-based attacks and increasingly employ other living-off-the-land techniques.** Malicious scripts declined as an attack vector by 11% in Q3 after dropping by 41% in Q2. Still, script-based attacks remain the largest attack vector, accounting for 56% of total attacks, and scripting languages like PowerShell are often used in living-off-the-land attacks. At the same time, Windows living-off-the-land binaries increased 32%. These findings indicate to Threat Lab researchers that threat actors continue to utilize multiple living-off-the-land techniques, likely in response to more protections around PowerShell and other scripting. Living-off-the-land attacks make up the most endpoint attacks.

- **Malware arriving over encrypted connections declined to 48%**, meaning just under half of all malware detected came via encrypted traffic. This figure is notable because it is down considerably from previous quarters. Overall, total malware detections increased by 14%.

- **An email-based dropper family that delivers malicious payloads comprised four of the Top 5 encrypted malware detections in Q3.** All but one of the variants in the Top 5 contained the dropper family named Stacked, which arrives as an attachment in an email spear phishing attempt. Threat actors will send emails with malicious attachments that appear to come from a known sender and claim to include an invoice or important document for review, aiming to trick end users into downloading malware. Two of the Stacked variants – Stacked.1.12 and Stacked.1.7 – also appeared in the Top 10 malware detections.

- **Commoditized malware emerges.** Among the top malware threats, a new malware family, Lazy.360502, made the Top 10 list. It delivers the adware variant 2345explorer as well as the Vidar password stealer. This malware threat connected to a Chinese website that provided a credential stealer and appeared to operate like a "password stealer as a service," where threat actors could pay for stolen credentials, illustrating how commoditized malware is being used.

- **Network attacks saw a 16% increase in Q3.** ProxyLogon was the number-one vulnerability targeted in network attacks, comprising 10% of all network detections in total.

- **Three new signatures appeared in the Top 50 network attacks.** These included a PHP Common Gateway Interface Apache vulnerability from 2012 that would result in a buffer overflow. Another was A Microsoft .NET Framework 2.0 vulnerability from 2016 that could result in a denial-of-service attack. There was also a SQL injection vulnerability in Drupal, the open-source CMS, from 2014. This vulnerability allowed attackers to remotely exploit Drupal without any need for authentication.

Given the many ways that threat actors are trying to gain access to sensitive information, organizations need a comprehensive, multi-layered cybersecurity strategy, with different types of security, including network, endpoint, Wi-Fi and identity protection working together to speed up threat detection and response processes. It's also important to remember that even the best defenses can be undone by social engineering attacks. Users need to understand that they are often the last line of defense preventing a malicious actor from penetrating an organization.

About the Author

Marc Laliberte is the Director of Security Operations at WatchGuard Technologies. Marc joined the WatchGuard team in 2012 and has spent much of the last decade helping shape WatchGuard's internal security maturation from various roles and responsibilities. Marc's responsibilities include leading WatchGuard's security operations center as well as the WatchGuard Threat Lab, a research-focused thought leadership team that identifies and reports on modern information security trends. With regular speaking appearances and contributions to online IT publications, Marc is a leading thought leader providing security guidance to all levels of IT personnel.

Marc Laliberte can be reached at https://www.watchguard.com/

Guardians of the Grid: Cyber-Secure Microgrids and the Future of Energy Resilience

The Crucial Role of Cyber-Resilient Microgrids

By Brian Jabeck, VP of Data Centers, Enchanted Rock

The vulnerability of major metropolitan power grids to natural disasters has become a pressing concern, but mother nature isn't the only thing threatening our grid these days. As society becomes more digitized, critical infrastructure faces increased exposure to cyber threats. And quite simply, there isn't enough power to go around so accessing new power is increasingly becoming a roadblock for data centers. One solution gaining traction is microgrids, which offer access to reliable power and ongoing electrical resilience for businesses and the government alike.

As our world becomes increasingly digitized, critical infrastructure is more exposed than ever before. Security experts describe a cyber-attack against the power grid as a form of asymmetrical warfare—a means of destroying a society by cutting off the delivery of food, water, healthcare, commerce, and communications. In essence, contemporary economies run on electricity, and without it, they seize up. It's vital to implement every security measure possible to prevent disruptions that could leave people without essential resources. What many don't realize is microgrids offer protection against cyberattacks and provide a promising avenue for enhancing grid security

As a source of onsite power generation during outages, microgrids ensure facilities and operations remain functional, but they can also help stabilize the grid during periods of grid stress. With their ability to operate independently from the main grid (islanding), microgrids can not only ensure continuous protection against cyber threats but also offer a flexible and efficient solution for the evolving energy

landscape. And in the case of extended outages, microgrids powered by natural gas ensure an additional layer of reliability when compared to potential delays or shortages of diesel fuel delivery. Natural gas is abundant, relatively clean-burning, and domestically sourced, making it a reliable option for energy generation.

The double-edged sword of AI and grid security

The emergence of AI has ushered in a new era for grid security, presenting a blend of promise and peril. On one hand, AI technologies offer a powerful toolset for bolstering grid resilience. Predictive analytics, powered by machine learning algorithms, can sift through vast troves of data from the grid and connected devices to preemptively detect and thwart potential threats. This proactive approach enables faster response times and more effective mitigation strategies in the face of cyberattacks or physical breaches.

Yet, the widespread adoption of AI also introduces new cybersecurity risks. As AI systems become increasingly interconnected and autonomous, they create avenues for malicious actors to exploit vulnerabilities. Adversarial attacks targeting AI models or data manipulation techniques pose a threat to the integrity of security solutions, potentially leading to false alarms or compromised decision-making. Moreover, concerns about algorithmic bias and transparency raise questions about the ethical implications of relying on AI for critical grid operations. While AI holds immense potential for advancing grid security, its deployment must be accompanied by both robust cybersecurity measures and electrical resiliency provided by natural gas microgrids. By embracing a comprehensive approach that prioritizes both innovation and risk mitigation, the industry can navigate the evolving threat landscape and safeguard critical infrastructure for future generations.

Data center microgrids as a blueprint for expanded infrastructure protection

The recent surge in AI has only intensified the skyrocketing growth and requirements of data centers. According to a recent Wall Street Journal article, the increased number of servers running on high-performance chips in an AI data center can result in a power draw of 50 kilowatts or more per rack, compared with roughly 8-14 kilowatts per rack in a conventional data center. As a result, power demand will continue to increase parallel to the AI landscape. With US data center consumption likely to go from 17 GW in 2022 to upwards of 35 GW by 2030, integrated microgrid systems are an ideal solution to fully support the additional infrastructure and increased energy requirements for these data centers.

And since microgrids serve as a blueprint for the expanded protection of critical infrastructure, their practical application for data centers provides a compelling model for enhancing resilience and reliability for all businesses and communities. These sophisticated energy systems offer valuable insights into the deployment of microgrids as decentralized energy generation and distribution, reducing vulnerabilities associated with centralized grids.

By decentralizing energy generation and incorporating resilient technologies, the data center microgrid model can be a guiding framework for bolstering the overall security and resilience of critical infrastructure. But ultimately, the power of public-private collaboration emerges as a crucial component

in the collective effort to build cyber-secure microgrids that ensure the resilience and reliability of our critical grid infrastructure.

Leveraging public-private collaboration to mitigate cyber risk

The ongoing collaboration between public-private partnerships such as government agencies, utility companies, energy companies and technology providers allow for the sharing of information, resources and expertise. This collective effort helps design effective strategies to protect critical grid infrastructure from threats. Incorporating natural gas into microgrid systems not only diversifies the energy mix but also provides a flexible and efficient solution for meeting energy demands. Advanced technologies can be leveraged to monitor and control natural gas-powered microgrids, enhancing their ability to withstand cyber threats. Additionally, the deployment of microgrids powered by natural gas aligns with efforts to reduce reliance on centralized grids, thereby mitigating vulnerabilities associated with large-scale infrastructure.

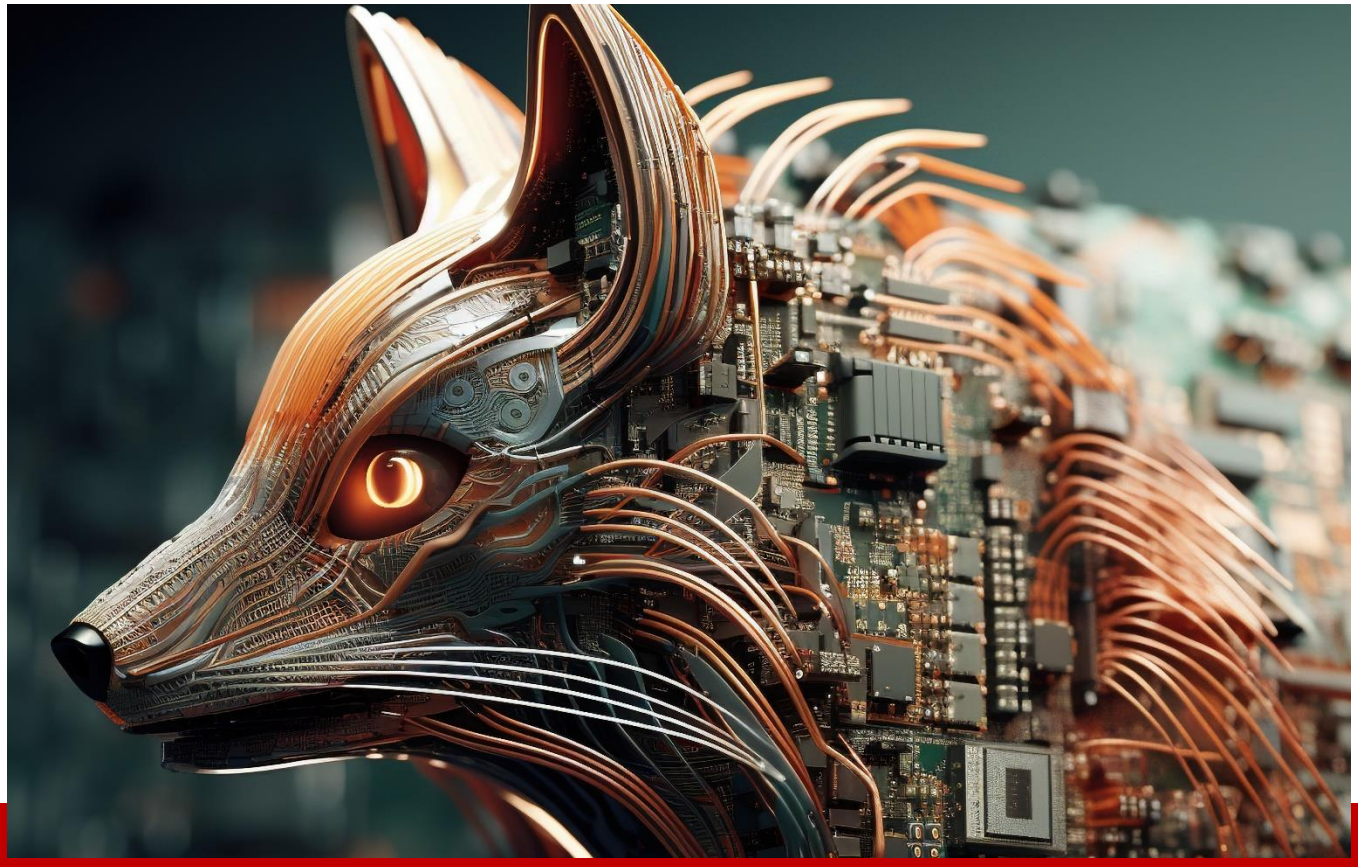
While there is no shortcut to effective cybersecurity, advanced microgrids can compensate for the loss of one or more control points. A cybersecure microgrid enables monitoring of internal communications and system processes to identify abnormal events during operations. This includes real-time alerts and the creation of security audit logs for operator awareness of the system's security posture, its level of availability, and potential anomalies, all without affecting the microgrid's operation. For true resiliency, cybersecurity protections must be built into the microgrid from its inception.

As the energy landscape continues to evolve, embracing natural gas-powered microgrids represents a proactive step towards building a more resilient and secure grid infrastructure. By harnessing the power of natural gas alongside advanced technologies and collaborative partnerships, we can mitigate the risks posed by cyberattacks and other disruptive forces, ensuring a reliable and sustainable energy future for generations to come.

About the Author

Brian Jabeck is VP of Data Centers, Enchanted Rock. He has helped many of the world's largest technology companies and energy providers find solutions to their power generation needs. In his current position Brian works with data center owners to leverage natural gas/RNG fueled dual purpose resiliency microgrids to deliver a backup power solution that also aligns with sustainability goals. Before joining Enchanted Rock in 2021, Brian worked for Caterpillar Inc. and Power Solutions International Inc. supporting standby power generation markets in North America and Europe. Brian's experiences include working with most of the global generator set manufacturers on diesel and natural gas solutions, as well as supporting key data center, contractor, and design engineering organizations.

Brian can be reached online at https://www.linkedin.com/in/brian-jabeck/ and at https://enchantedrock.com/



Stop Chasing the AI Squirrel and Patch… Just Patch

By Craig Burland, CISO, Inversion6

In the contemporary technological landscape, the allure of advanced artificial intelligence (AI) systems often captivates the collective imagination of the tech industry and beyond. Stories of deepfakes, such as the recent incident where a CEO appeared to say compromising things during a virtual call—engineered through sophisticated AI—fuel anxieties and fascinations. However, while such scenarios grab headlines and provoke fears about the future of digital security, they distract from a far more mundane and immediate threat: the lack of basic cyber hygiene.

Based on the latest Verizon 2024 Data Breach Investigations Report (DBIR), the percentage of breaches directly attributable to AI was 0%. That's right. Zero. The percentage of breaches directly attributable to exploitation of vulnerabilities was 15%, having grown by 180% over the previous twelve months. The other two big contributors: credential theft and phishing. Looking beyond just data breaches, the Ponemon Institute found that 57% of cyberattack victims stated that applying a patch would have prevented the attack. 34% say they knew about the vulnerability before the attack. This statistic reveals a critical disconnect in organizational priorities and resource allocation. Companies are so enthralled by

the specter of high-tech AI threats that they overlook the foundational practices that protect against most cyber threats: patch management. While the DBIR doesn't have data related to the percentage of C-Levels keenly interested in credential loss or patching compliance, I doubt it matches the risk.

Patching isn't glamorous. It doesn't involve cutting-edge technology or revolutionary algorithms. Instead, it requires diligent, ongoing allocation of resources and a disciplined commitment to routine. In other words, it's a grind. But despite its lack of allure, patching is one of the most effective defenses against cyber-attacks. Regular updates close security holes and fix bugs that could be exploited by attackers. Even those leveraging AI. Patching is the equivalent of changing the oil and rotating tires of your car. While discussing the latest car hack from Black Hat might make for good dinner conversation, the two conversations must not be mutually exclusive. "Honey, I've upgraded our garage with metal mesh fencing to prevent OTA updates." "That's great, dear. Did you change the oil? It's been 30,000 miles." "That's not going to stop the OTA updates!"

The emphasis on the dangers of AI steals time and focus from the real risks threatening organizations. Take, for example, the recent deepfake incident involving a CEO in an AI-generated virtual meeting, including fake speech and virtual attendees. Although such an event is sensational and its implications on misinformation and security are profound, it is a very rare, hard-to-scale attack compared to the daily occurrences of data breaches and hacks facilitated by unpatched systems. Diverting attention from foundational cybersecurity to the threat du-jour misses a core tenet of risk management. Risk is likelihood multiplied by impact. Currently, the likelihood of a direct AI incident is nearly zero while the likelihood of a breach due to unpatched vulnerabilities is significantly higher.

To focus on real, rather than imagined risk, senior leaders should assign themselves to a committee dedicated to the fundamentals of cybersecurity. This committee would prioritize developing and enforcing policies that ensure regular updates and patches are applied promptly. It would ensure sufficient resource allocation. It would support planned business disruption like maintenance windows. It would champion asset lifecycle investments. It would ask questions like, "how are we securing our SaaS applications?", "are we evaluating our third parties?", and "are our products secure?". This committee would also oversee the training of staff to recognize the signs of an attack and understand the importance of updates, creating a culture of security that permeates every level of the organization.

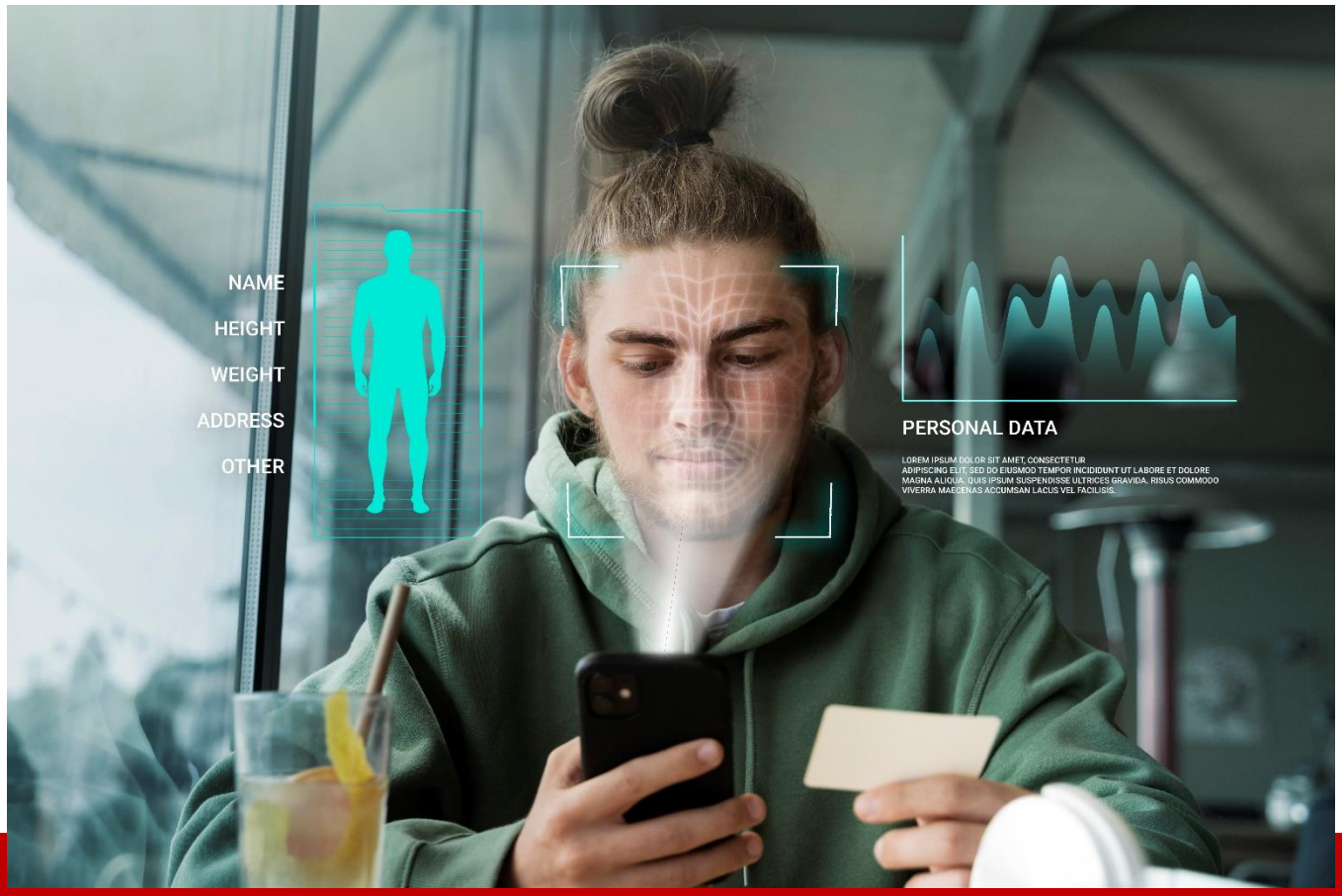
By focusing on practical and immediate improvements in cyber hygiene, companies can significantly reduce their vulnerability to most cyber threats, business disruption, investor concerns, and regulatory peril. This shift in focus does not mean ignoring the potential risks posed by AI and other emerging technologies, but it does mean addressing the risks that can have a material impact in the here and now. Consider all the recent discussion about the SEC rules about reporting incidents or the lawsuits against CISOs for misreporting risks. Those potential pitfalls are rooted in real risks, present in the everyday operation of organizations.

The tale of the deepfake CEO serves as a stark reminder of the dual threats facing modern organizations: the tangible and the theoretical. While it is necessary to prepare for the future and innovate to stay ahead of potential threats, this should not come at the expense of addressing present and pervasive risks. Patch management may not be headline-grabbing, but it is a fundamental aspect of maintaining security in a digital world. Organizations must stop chasing the AI squirrel and focus on the essential tasks at hand.

By doing so, they can better protect their organization, ensure stakeholder value, and create a more resilient digital environment.

About the Author

Craig Burland is CISO of Inversion6. Craig brings decades of pertinent industry experience to Inversion6, including his most recent role leading information security operations for a Fortune 200 Company. He 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. Craig can be reached online at LinkedIn and at our company website http://www.inversion6.com.



Digital Identities Have Evolved -- Cyber Strategies Should Too.

By Trevor Hilligoss, VP of SpyCloud Labs at SpyCloud

The scale of identity exposure has increased significantly, with over 90% of surveyed organizations reporting an identity-related breach within the last year. These attacks have long-lasting consequences – SpyCloud's 2024 Identity Exposure Report found that the average digital identity appears in as many as nine breaches and is associated with 15 breach records.

The escalating threat to identities has forced organizations to adopt novel approaches and tools to bolster their cyber defenses, such as passkeys. However, despite these efforts, criminals are still managing to evade these protections through sophisticated, next-generation identity attacks. Information saved by browsers, like session cookies, API tokens, or form-fill data, enable criminals to exploit these attack methods and bypass traditional authentication protections to seize control of a user's account.

To counter these evolving threats, organizations must not only broaden their understanding of what constitutes a digital identity but also adopt proactive measures to defend against emerging attack vectors.

What's in an Identity?

A user's digital identity is no longer limited to an email - or username - and password. With the ever-increasing amount of data we share online, criminals have access to an ever-increasing pool of personally identifiable information (PII) available for potential attacks.

SpyCloud found over 200 unique types of personally identifiable information (PII) on the darknet in 2023, including birthdates, credit cards, passport details and social security numbers. User identities have expanded to include hundreds of data types, like national ID's, location information, social handles and more. Cybercriminals are leveraging the resulting datasets to dramatically increase the scope of their attack patterns.

By combining seemingly disparate data types, attackers can piece together information and perpetrate cybercrimes like identity theft, fraud, and next-generation account takeover. Our research suggests that over 74% of people exposed in breaches reused compromised passwords, increasing the likelihood that a lucky criminal strikes gold.

As our digital identities expand beyond legacy account-based credentials, our protections must shift to stay relevant to new trends.

"C is for cookie and cookie is for me." – Cookie Monster

Criminals' use of users' session cookies to perpetrate sophisticated cyber attacks is another trend resulting from expanded digital identities. Over 20 billion cookie records were exposed on the darknet last year, with an average of more than 2,000 records stolen per malware-infected device. These cookies equip criminals with all the information they need to carry out attacks, like session hijacking, which is when criminals seize control of an existing online session using stolen cookies.

Often obtained via infostealer malware, attackers put these cookies into so-called "anti-detect" browsers, which allow them to bypass traditional authentication protections and mimic users, especially when combined with information like the victim's IP address and other host information. These attacks provide threat actors with the same rights and permissions as the legitimate user, making them exceedingly difficult to detect.

Passkeys and multifactor authentication (MFA) don't protect against these attacks—session hijacking bypasses the authentication process entirely. And even sophisticated methods of detecting anomalous behavior, like device fingerprinting, can be bypassed using criminal residential proxies and other cybercrime enablement services. With malware-driven attacks rising in popularity, organizations need to understand the threat malware poses and how to mitigate it.

Malware is Exposing Identities Like Never Before

Over 61% of data breaches in 2023 were malware-related. While information stealing malware is not a new concept, it has never before been as accessible and feature-rich as it is today.

Infostealer malware poses a considerable threat since it can exfiltrate large volumes of high-quality data in seconds. Typically sold as malware-as-a-service, or MaaS, these stealers are often bundled with services aimed at making the malware harder to detect by antivirus and other endpoint security solutions. This ability to bypass these solutions can leave little to no trace of the bad actor's existence on a victim's device, and few network-based indicators to pursue. SpyCloud found that in 2023 alone, the average digital identity had a 1 in 5 chance of already being a victim of an infostealer malware infection.

The sheer volume and diversity of infostealer families active on the darknet further exacerbate the threat. More than 52 infostealer families were active on the darknet in 2023, with four entirely new families discovered in the last quarter of the year.

That said, it's not just the scale of these attacks that poses a risk to users; it's also the nature of the targeted data. In the current cyber landscape, safeguarding against increasingly sophisticated identity threats requires a new approach.

Next-generation protections

Current malware remediation strategies focus on addressing malware-compromised devices but neglect valuable identity data like session cookies and other PII already exposed on the darknet. If not remediated, criminals will sell or trade this data on the darknet to facilitate additional cybercrimes long after devices have been wiped.

Organizations need a robust post-infection remediation strategy that addresses and accounts for data stolen in an attack. By proactively monitoring the darknet for compromised data, organizations can get a more holistic look at their attack surface. Security teams can then force users to reset exposed data, such as session cookies, and cut off criminals' entry points before they can cause harm.

IT teams must prioritize solutions offering heightened visibility that tackle security vulnerabilities stemming from malware. By shifting from a device-centric to identity-centric malware remediation strategy, security teams can proactively mitigate the risks of infostealer malware, preserving brand reputation and companies' bottom line.

About the Author

Trevor is the Vice President of SpyCloud Labs. Trevor served nine years in the U.S. Army and has an extensive background in federal law enforcement, tracking threat actors for both the DoD and FBI. He is a member of the Joint Ransomware Task Force and serves in an advisory capacity for multiple cybersecurity-focused non-profits. He has spoken at numerous US and international cyber conferences, holds multiple federal and industry certifications in the field of cybersecurity, and is a recipient of the President's Volunteer Service Award for volunteer service aimed at countering cyber threats.

Trevor can be reached online at SpyCloud's website https://spycloud.com/

Pioneering the New Frontier in AI Consumer Protection and Cyber Defense

By Magnus Tagtstrom, Corporate VP Emerging Tech and GM Europe of Iterate.ai

In a groundbreaking move, the first state in the U.S. has passed comprehensive legislation aimed at protecting consumers from the potential risks associated with AI. The new Utah Artificial Intelligence Policy Act (AIPA) was signed into law by Governor Spencer Cox and took effect May 1. The new law requires transparency when businesses use AI. Should the AI deceive consumers, then businesses could be fined an administrative fine of up to $2,500 and/or civil penalties up to $5,000. This legislation, pioneering in its approach, centers on the crucial intersection of AI development and cyber defense, marking a significant step forward in the ongoing efforts to safeguard personal and national security in the digital age.

At the heart of this legislative push is a keen awareness of the cyber threats that accompany the advancement of AI technologies. With AI's growing role in various sectors, including finance, healthcare, and personal devices, the potential for cyberattacks leveraging AI systems has escalated. The legislation introduces mandatory cybersecurity measures for AI developers and users, aiming to fortify the state's cyber defenses against sophisticated AI-powered threats.

These measures include rigorous testing of AI systems for vulnerabilities, regular updates to address emerging cyber threats, and compliance with state and federal cybersecurity standards. Recognizing the dynamic nature of both AI technology and cyber threats, this mandate ensures that AI systems undergo continuous scrutiny. Testing is designed to evolve alongside advancements in AI, with the objective of preemptively identifying potential security breaches before they can be exploited. This ongoing vigilance is complemented by the requirement for regular system updates, which serve as an essential defense mechanism against newly emerging cyber threats. These updates are not merely reactionary but are part of a proactive strategy aimed at maintaining the highest levels of system integrity and resilience against cyber attacks.

Central to ongoing legislation will also center around consumer protection. Recognizing the opaque nature of many AI operations, the law mandates clear disclosures about the use of AI in consumer products and services, including the scope of data collection and the purpose of AI analysis. This transparency is designed to empower consumers with the knowledge to make informed decisions about their engagement with AI-powered platforms.

Additionally, the legislation addresses the critical issue of consent, ensuring that consumers have a say in how their data is used by AI systems. This is particularly relevant in light of recent concerns over AI-driven data harvesting and profiling practices. The passage of this legislation sets a precedent for other states and potentially at the federal level, highlighting the importance of regulatory frameworks in the era of AI. It reflects a growing recognition of the dual nature of AI as a tool for innovation and a potential vector for cyber threats.

Industry experts have lauded the legislation as a necessary step in fostering a safer digital environment, encouraging responsible AI development, and promoting public trust in emerging technologies. Conversely, some critics argue that stringent regulations may stifle innovation and deter AI advancements. Nonetheless, the prevailing sentiment is one of cautious optimism, with a focus on balancing progress with protection.

Looking Ahead

As AI continues to evolve, the challenge for lawmakers and the tech industry will be to adapt regulatory approaches to keep pace with technological advancements while ensuring robust cyber defense mechanisms are in place. The pioneering state's legislation serves as a template for future regulatory efforts, emphasizing the need for a collaborative approach involving government, industry, and civil society to navigate the complexities of AI governance.

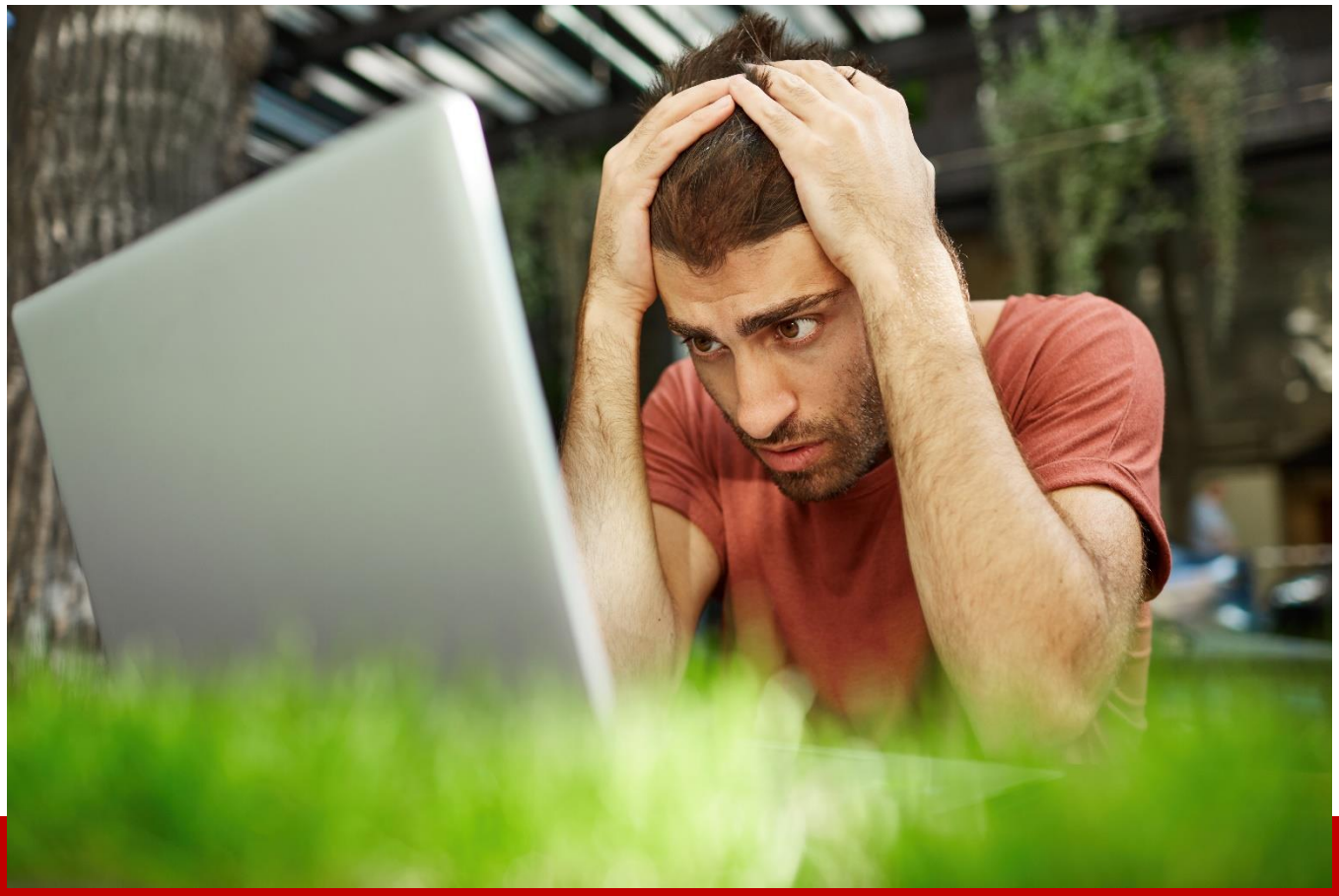
This legislation marks a significant stride towards establishing a secure, transparent, and consumer-friendly framework for AI use. At the core of future legislative efforts, cyber defense in the digital age will be a major aspect, creating a foundation to harness AI while mitigating its risks. The emphasis on cybersecurity within legislative efforts will be crucial, serving as both a safeguard and a catalyst for the responsible harnessing of AI's capabilities. This approach ensures not only the protection of personal and national security but also fosters an environment where the innovative potential of AI can be explored and realized safely and ethically. By prioritizing the integration of comprehensive cyber defense

strategies, this legislation sets a precedent for how we can navigate the challenges and opportunities of AI, positioning it as a key component in mitigating risks and enhancing the trust and safety of digital ecosystems for all users.

About the Author

Magnus Tagtstrom brings Iterate a rare combination of proven business acumen and deep technology understanding," said Brian Sathianathan, co-founder and CTO at Iterate.ai. "He's an award-winning leader—several times over—who has had an immense and lasting impact on innovation at Alimentation Couche-Tard. We also believe that his perspective, working closely with Interplay on the customer side, will be invaluable to both the low-code platform decisions we make and to our go-to-market strategy in Europe. We're excited to welcome Magnus, a longtime partner to Iterate, to the team.

Magnus Tagtstrom can be reached online at https://www.iterate.ai/



5 Reasons IGA Programs Fail

By Jackson Shaw, CSO, Clear Skye

Identity governance and administration (IGA) is a critical part of modern business. It's one of the single most important pieces of creating and balancing a productive and secure work environment. With a reputation like that, IGA should be the star of the show. Yet, for many, it's simply a box to check or an afterthought. Perhaps that's why so many IGA programs fail. But there's no time like the present to turn it around and start realizing true business value from your identity solution.

Make no mistake, running a successful IGA program requires effort. That effort, when done right, can both protect and accelerate your business. At a time when data is both a prized asset and a potential liability, IGA is the key to safeguarding one and unlocking the other. So, as you embark on your IGA journey, consider these five common roadblocks to a successful identity program and how you can flip the script.

1.) Unrealistic Expectations

Whether its vendors overselling their capabilities or the belief that Rome was built in a day, unrealistic expectations are bound to leave you disappointed. The most impactful way to demonstrate progress is to show broad value to a large audience immediately. When you consider a time not too long ago when you had to spend 30 minutes on the phone with the HelpDesk to reset your password, this isn't as hard as it may sound. Set up your IGA initiative, deploy it, make it widely available, and above all, make sure it makes work easier for users. When employees understand and see the value in new processes, it can help facilitate more complex IT projects where the results may not be as visible.

2.) Forced Change

You may not have been in the market to upgrade your legacy on-prem IGA solution, but what if your vendor is migrating to the cloud? Even in the name of digital transformation, a massive tech overhaul can feel like anything but an improvement. So, do you grin and bear it or seek out another IGA solution entirely? While it seems daunting, choosing a new IGA solution can be a strategic opportunity to streamline productivity and strengthen security. Those who choose the latter approach should explore leveraging their existing IT competencies and tech stack to see if there's a solution that works with their current systems and processes.

3.) Poor Support

Many identity vendors address the high cost of deployment and management by offering SaaS versions of their application. But these solutions lack feature parity with previous solutions, and are less customizable and functional due to cloud architecture. This means if you're forced to upgrade, you're also forced to adjust business processes to fit what's available in the new solution. When you run your IGA program on your existing business platform, you remove the need to choose between security, flexibility, and maintenance. This approach provides not only a common user interface (UI) across a variety of IT and business areas, but a strong cloud architecture and streamlined workflows.

4.) Biting Off More than You Can Chew

The average business uses 371 SaaS applications (Productiv). The role of IGA is to maintain security and minimize risk of said apps. Yet, few have full connectors to bring them into your IGA solution. Instead, most are managed by IT Service Management (ITSM) processes or outside IT altogether. Not only is this a huge undertaking, but it leaves organizational silos and security gaps. Automating IGA tasks can help streamline efforts to ensure all applications are under governance in one single system or platform. By coupling IGA and ITSM with automated workflows, IT teams can bridge once disconnected systems and better manage all enterprise applications.

5.) Politics

Tale as old as time: a new executive comes in and brings their preferred team and vendors with them. This isn't always a bad thing, but consideration must be given to how this fits into an existing organizational framework. Ripping and replacing for the sake of making your mark can lead to frustrated employees and unproductive processes that equate to more headaches than results. Be intentional about the solutions you choose—especially identity ones, which touch every aspect and person involved with your business.

The failure of IGA programs can be attributed to a variety of factors. Without proper alignment with business objectives, ineffective implementation, and a lack of immediate value-add, IGA initiatives will continue struggling to gain traction and deliver the intended benefits. To address these challenges and maximize the success of identity programs, organizations must get real about their expectations, plan strategically, be adaptable to change, and go one step at a time. By addressing the common IGA missteps, organizations can enhance their security posture, streamline compliance efforts, and unlock the full potential of their IGA investments.

About the Author

Jackson is the CSO at Clear Skye. He began his identity management career as an early employee at Toronto-based Zoomit Corp., the pioneer in the development of meta-directory products who Microsoft acquired in 1999. While at Microsoft, he was responsible for product planning and marketing around Microsoft's identity & access management products including Active Directory and Microsoft Identity Manager. Jackson has held various senior product management and marketing roles since Microsoft including Vintela, Quest Software, Dell, One Identity, and Forcepoint. He studied computer science at the University of Ottawa, Canada. Jackson can be reached online at jackson@clearskye.com, LinkedIn, Twitter, and at our company website https://clearskye.com/

How the Newest Tech Changes Cybersecurity Needs in the Legal Industry

Responsibly Adopting Technology to Improve Law Firm Productivity

By Robert Scott, IT Attorney & Chief Innovator, Monjur

Lawyers face incredible pressure in their jobs to perform accurately and quickly. Thankfully, technology has been introduced that now allows legal professionals to significantly streamline their processes and improve efficiency while meeting their clients' needs.

However, many of these technologies introduce ethical and security considerations that lawyers must consider before integrating these tools into their operations. As a result, it becomes essential for lawyers to prioritize responsible practices when adopting these technologies in pursuit of the benefits they offer — otherwise, they could potentially expose their firms and clients to serious cybersecurity risks.

How technology has impacted cybersecurity in law

Technology has long been influential in many of the back-end administrative tasks of running a law firm, but has only in recent years become more prominently used in firms' cybersecurity measures. For example, technology has been used to ensure secure document management and transaction

processing, and as it has evolved, these platforms become more secure and convenient. Platforms now exist that allow lawyers to collect e-signatures, enter into click-wrap agreements, and obtain browse-wrap consent at once to ensure that lawyers have everything they need to enter contracts quickly and simply.

Another technology that has been beneficial in the legal industry is cloud platforms, which allow legal teams to collaborate remotely and ensure consistent accessibility. With the help of this technology, lawyers can access essential documentation on demand and expand teams around the world.

The advantages that technological evolutions like this provide to clients are tremendous, as clients can now effectively have more people working for them to help win their cases. Advanced cybersecurity measures allow these platforms to remain secure by transmitting information and documents in ways that protect clients' sensitive and confidential data.

Artificial intelligence technology in the legal sector

However, perhaps the most important paradigm shift we see in the legal sector, like virtually every industry, is the recent widespread embracing of artificial intelligence (AI). Although the law field is often seen as fundamentally "human," many day-to-day tasks that were once left to humans can now be automated and streamlined using AI. For example, many lawyers have seen success in applying AI technology to their case research and analysis processes, allowing them to spend more time on what matters most: working for their clients.

Technology like this has the exciting potential to fundamentally change how lawyers complete their duties — particularly the more monotonous aspects of their jobs. In some use cases, AI models could significantly improve the speed, efficiency, and accuracy with which lawyers complete tasks. For example, in the legal review process, an AI model can be trained to scan for differences in two contract drafts, alerting lawyers to language that may require specific attention and review.

Nevertheless, an element of humanity must be maintained in the legal sector when using advanced tools like AI. Artificial intelligence is still a relatively new technology and, like any fledgling technology, is often flawed and prone to make mistakes. Thus, it is essential to have a skilled human lawyer review any of the work completed by an AI platform. After all, lawyers regularly handle sensitive, confidential information and make decisions that alter the course of lives. Putting these processes into the hands of an artificial intelligence model without human oversight is incredibly dangerous and could potentially lead to drastic consequences.

As such, lawyers must also adopt responsible ethical practices regarding data security in artificial intelligence, as many AI algorithms use the data it is fed by users as part of their training process. Especially when dealing with sensitive or confidential information, lawyers must be intimately familiar with all terms of use and privacy policies for the platforms they use to understand how their data (and their clients' data) is being collected, stored, and used. Furthermore, it is necessary to implement strict access control policies to ensure that unwanted parties cannot access the data in these programs.

Responsibly shaping the future of technology in the legal sector

Still, when it comes to adopting new technologies in fields as complex as the legal sector, it's not just about staying ahead of the curve — it's about defining the curve. How pioneers integrate artificial intelligence into their operations today will shape and determine how the technology can and will be used in the future. For example, current legislation and regulations that are being introduced surrounding the use of AI are informed by discoveries being made through current use cases.

Therefore, lawyers who adopt new technologies improve not just their own work but also their client service and the legal landscape for future generations of legal professionals. Now is the time to get on the ground floor with innovation by embracing new technologies like document management, cloud platforms, and AI, as they will only help lawyers increase the productivity and efficiency of their firms.

About the Author

Robert Scott is a thought leader in managed services and cloud law serving as the Chief Innovator for his latest venture, monjur, with a mission to redefine legal services. Robert has been recognized as the Technology Lawyer of the Year by Finance Monthly and carries an AV Rating as Preeminent from Martindale Hubbell. He represents major corporations in strategic IT matters including cloud-based transactions, managed services contracts, data privacy, and cybersecurity risk management. Robert is licensed to practice law in Texas and holds memberships in several professional associations, including the Dallas Bar Association and the Managed Service Providers Alliance Board. He regularly shares his insights on the MSP Zone podcast and is a frequent presenter at industry conferences, discussing various subjects such as cybersecurity, regulatory compliance, and AI contracts. His depth of knowledge and commitment to his field make him a trusted advisor in the rapidly evolving landscape of technology law. Robert can be reached online at rscott@scottiplaw.com, on LinkedIn, and at his company's website, https://monjur.com.

Deep Dive: Unveiling the Untold Challenges of Single Sign-On (SSO) Management

By Chetan Honnenahalli

Single Sign-On (SSO) serves as the linchpin connecting corporate networks, facilitating seamless access to various web applications without the need for repeated login credentials. However, there are several untold challenges that Identity Access Management and Cybersecurity experts face every day across the world in maintaining a stable SSO infrastructure. Within this article, drawing upon my extensive experience in Identity Access Management and Security, I aim to provide a comprehensive walkthrough for establishing the necessary infrastructure for a stable SSO implementation that works consistently and avoids surprise failures.

What is SSO and How Does it Work?

SSO makes life easier by letting users hop from one app to another with just one click, no need to type in their login details every time. It's like having a magic key that unlocks multiple doors! Basically, there are two main players in this game: the Identity Provider (IDP) and the Service Provider (SP). The IDP is where you're already logged in - your starting point, while the SP is where you want to go - your destination. And when it comes to SSO, there are two popular ways it can happen: IDP-initiated SSO and SP-initiated SSO.

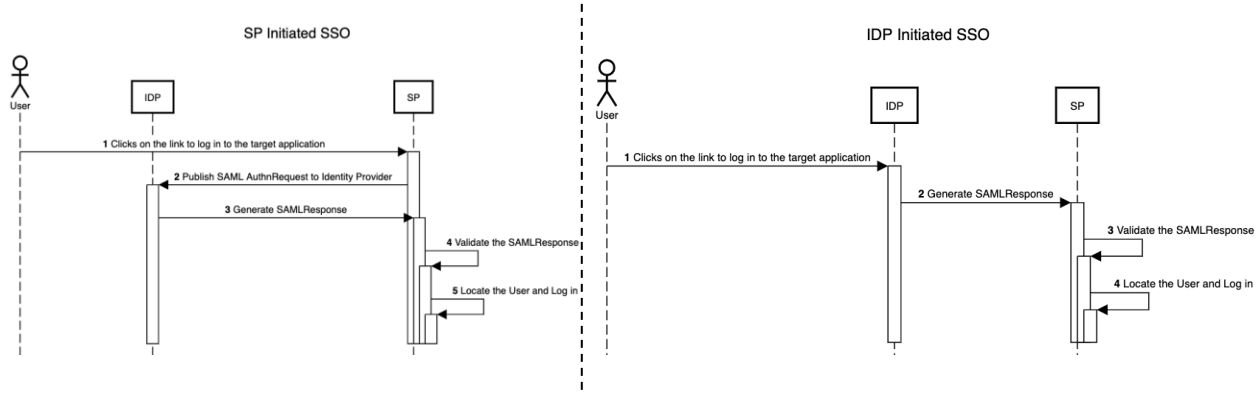


Figure 1: Different Types of SSO Mechanisms

In both cases, the IDP issues a Security Assertion Markup Language (SAML) token containing a user identifier, which the SP verifies for authenticity. Using this identifier, the SP finds the user in its database and grants access for login.

Key Components of SSO

User Provisioning

For a seamless SSO transaction to occur the user's identity must exist in both the systems. This can be done either through a proactive database sync between the two software systems ahead of time or new users can be provisioned on demand when a SSO request is received by the Service Provider (also called Just In Time provisioning).

SAML (Security Assertion Markup Language) Token Verification

The SAML token includes a signature, user ID, and timestamp for token generation. A private-public key shared certificate generates the signature, requiring an exchange between IDP and SP administrators beforehand. The IDP holds the private key, and the SP holds the public key. Upon receiving a SAMLResponse, the SP verifies the signature using its public key to authenticate the token. Timestamps are also examined to prevent replay attacks by malicious actors who may acquire the token through a man-in-the-middle attack.

Untold Challenges Faced in Practice

Inconsistent Terminology & Incompatible Signatures

Various SSO vendors offer solutions, with some firms opting to develop their own. This diversity results in inconsistent terminology across vendors. For instance, the URL receiving the SAMLResponse token (step 2 in Figure 1) goes by various names like Assertions Consumer URL, SAML Post URL, and SAMLResponse URL. Moreover, different vendors employ different methods for signing the SAMLResponse token. While some sign only the payload (user identifier, timestamps), others sign the entire token. If the signature expectations of the Service Provider (SP) and Identity Provider (IDP) don't align, SSO transactions can fail.

Corporate Firewall Misconfiguration

Corporate networks restrict traffic to known IP ranges, causing SSO failures if an IDP or SP's IP falls outside the allowed list. Additionally, proxies in corporate networks sanitize web traffic, sometimes resulting in incomplete or missing request payloads during exchanges between IDP and SP, further impacting SSO functionality.

Clock Drift

Clock Drift is a phenomenon where a server's clock goes out of sync with natural time and begins to lag. If either SP or IDP has servers that have drifted, then the timestamps published in the SAMLResponse token appear stale to the SP, causing it to suspect malintent and reject the token, in turn causing the SSO to fail.

It is important for the SP and IDP's administrators to know and account for these factors before SSO transactions can occur in order to save countless engineering hours spent in troubleshooting SSO failures.

Other Often Ignored Facets of Supporting SSO

Improper Certificate Management

The private-public key pairs exchanged between IDP and SP have expiration dates for security reasons. When a certificate expires, it causes SSO failures due to invalid signatures and leads to board scale service unavailability. To prevent this, certificates must be tracked, renewed, and deployed before expiration. Storing certificates externally, rather than within the application, allows for easy replacement and validation. Caching certificates minimizes I/O for fetching, with the cache invalidated upon expiration.

Lack of Troubleshooting Tools

SSO is essential for onboarding new partners, typically occurring as the final step in the sales cycle. Onboarding is often managed by non-technical personnel, so providing self-service tools empowers them

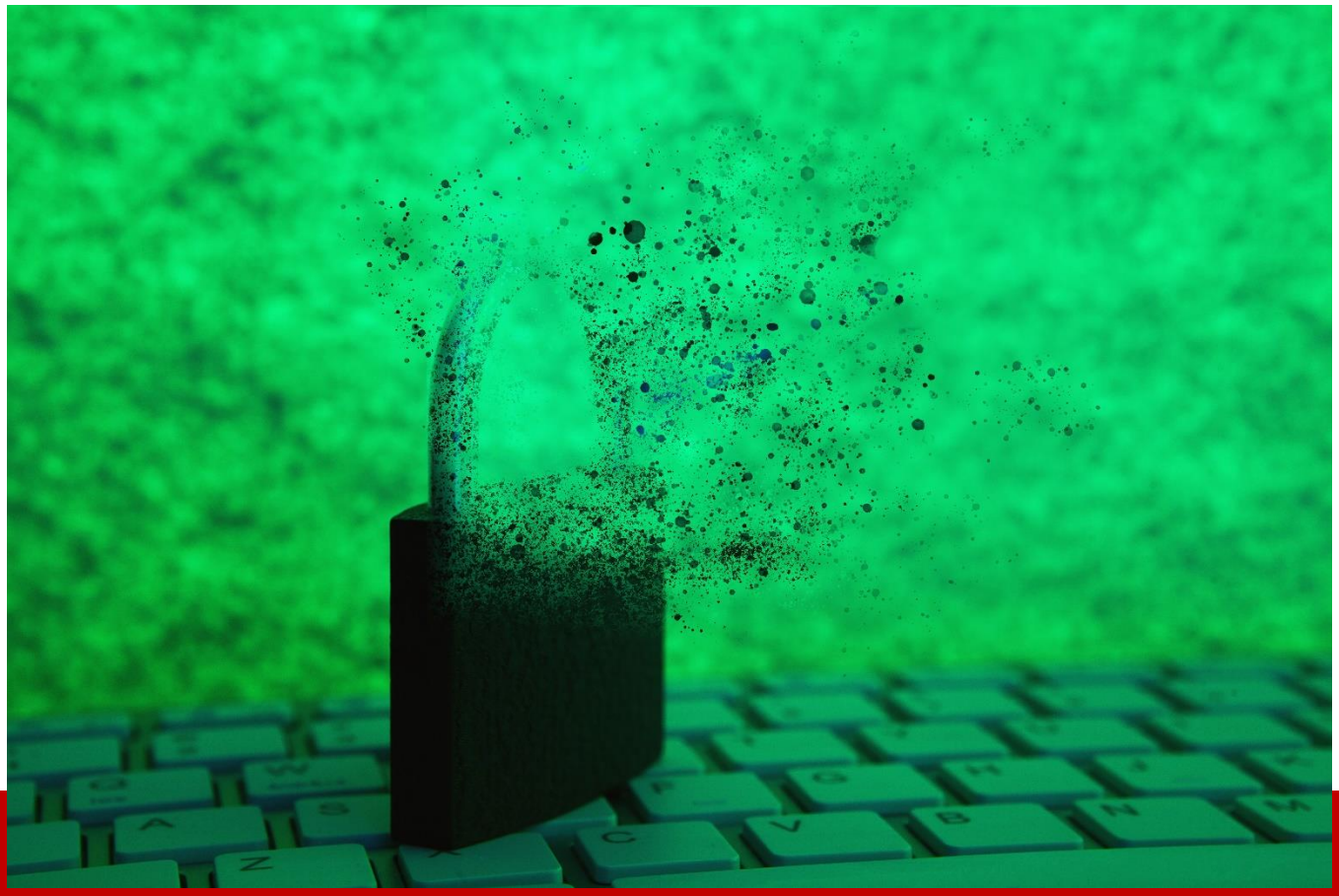
and streamlines the process. A web-based interface tracking SSO requests and responses, and highlighting issues, facilitates smoother onboarding.

Conclusion

Single Sign-On accelerates business partnerships and rapid adoption of online services globally. Yet, managing the SSO infrastructure can be complex. This document outlines measures to simplify SSO administration worldwide.

About the Author

Chetan Honnenahalli is a Cybersecurity and Identity Access Management (IAM) expert with more than 15 years of industry experience in companies such as American Express, Zoom and Meta. Chetan can be reached online at https://www.linkedin.com/in/hschetan/



Sheltering from the Cyberattack Storm

By Nick Lines, Security Product Expert, Panaseer

As we move towards the summer and the promise of sunnier weather, it's worth noting that the cybersecurity industry has seen more rain than sunshine recently. A slew of high-profile breaches have had a stark impact on the business landscape and people's daily lives, from emails exposed in the wake of Microsoft's email breach, to personal data stolen as part of the MOVEit hack. Regulators have become frustrated and stricter with their requirements and enforcement, with the SEC now laying the blame for security incidents at CISOs' feet. This is raising the stakes of an already high stakes game, and if the cybersecurity industry continues on this path, the storm will continue.

Analysis of the most potent recent attacks shows that breaches – largely – fall into three distinct buckets. There are the genuinely sophisticated attacks that are conducted by well-resourced adversaries – highly established groups or state-backed attackers. Then there are the industrialized attacks, which require technical skill, but don't operate on the same level of complexity and tend to be less targeted. Finally, there are the opportunistic attacks, which are often automated and have a low bar for entry.

All three have their own intricacies, and while the methods for defending against them may vary, there is one common theme – ensuring the right controls are in place and have been deployed effectively. In the first of this two-part series, I'll focus on the sophisticated attacks, before turning to industrialized and opportunistic attacks in the next piece.

The sophisticated attack cyclone

Sophisticated attacks are the hardest to remediate, and often have a broader and longer lasting impact. The Microsoft email hack in July 2023 is a prime example. It was one of the most tenacious attacks of the last few months, which ultimately allowed the adversary access to almost any email hosted on Microsoft 365. This included many government and defense departments globally as well as private businesses – both large and small.

In this case, state-sponsored threat actors were responsible, using a mix of exceptional techniques mixed with traditional Tactics, Techniques and Procedures (TTPs). To Microsoft's credit, it was initially open about the attack, even detailing how it occurred, shedding light on multiple points of failure, going back as far as 2021. It has since updated this blog, scaling back on its original hypothesis, but still pointing to operational issues as the cause.

The original blog pointed to multiple points of failure – both in the tech and operations – that left the front door wide open to the attackers. This was confirmed by a US Department of Homeland Security's Cyber Safety Review Board (CSRB) review of the incident, which was conducted due to the global significance of the attack. What remains clear is that there were multiple stages where this devastating attack could've been interrupted to limit its impact, or even stop it in its tracks.

But the attack shows that nobody is immune to cybercrime, and that a determined, well-resourced attacker will compromise even the biggest organizations that pride themselves on their security.

Sheltering from the storm

However, even with sophisticated attacks, organizations can take steps to secure themselves by ensuring a zero trust strategy. But achieving zero trust is hard, and can be overwhelming when applied to every individual, and every single device, application and scrap of data the organization owns. So organizations should prioritize the systems that would benefit most from zero trust initiatives first.

Understanding what resources and which users are critical to the business will allow security teams to set realistic goals and outcomes when looking to deploy zero trust initiatives. For instance, zero-trust might not be a priority for the machine displaying menu options in the staff canteen. But it will be for ensuring privileged users with access to business-critical data can still do their jobs.

Organizations' first goal should be to ensure they have the data to fully understand their landscape, how users interact with it, and where the greatest risks are. Armed with this they can create measurable objectives to roll out a zero-trust strategy, starting where it's needed the most, showing success and then expanding the initiative.

Inclement weather inbound

While these sophisticated attacks are the rarest due to the skills required to launch them, they are often the most devastating, and the hardest to defend against. But organizations – particularly enterprises – must be prepared for all three types of attack, as they're likely to encounter them all. In the next piece, I'll be covering the human-operated and opportunistic attacks that occur more regularly, but are just as potent, and how to defend against them.

About the Author

Nick Lines, Security Product Expert, champions Panaseer's unique value and ensures they're helping solve the biggest challenges in cybersecurity. He's worked for multinational systems integrators and consultancies in roles including developer, technical sales, and offering management, and previously spent a decade at Microsoft. Nick can be reached online at LinkedIn and at our company website https://panaseer.com/.

Unlocking the Power of Behavioral Cloud Native Threat Detection and Response

By Jimmy Mesta, Co-founder and CTO, RAD Security

Behavioral detection and response is not a new concept, and the top three detection and response players command a combined market capitalization of $100 billion. But the rise of cloud native environments has presented both opportunities and challenges in this area. As organizations increasingly embrace microservices architecture, containers, and orchestration tools like Kubernetes to build scalable and resilient applications, the need for effective threat detection and response mechanisms has become paramount. So what does your organization need to know about behavioral cloud native threat detection and response?

Understanding Cloud Native Environments

Before diving into behavioral threat detection, it's crucial to grasp the essence of cloud native environments. Unlike traditional legacy applications that are tightly bound to specific servers or VMs, cloud native applications are designed to be agile, flexible, and adaptable to cloud infrastructures. They leverage microservices, containers, and orchestration tools to achieve scalability and resilience, making them well-suited for dynamic cloud environments.

However, this flexibility comes with its own set of challenges, especially in terms of security. A study revealed that a staggering 90% of teams using containers and Kubernetes experienced security incidents in their environments, highlighting the urgent need for robust threat detection and response strategies tailored to cloud native ecosystems.

The Evolution of Threat Detection

Traditional threat detection methods, such as signature-based approaches, have proven inadequate in cloud native environments. Signature-based methods rely on predefined rules to detect known threats, but they struggle to keep pace with the rapid onslaught of new threat actors and require thousands of signatures to every known threat. This leads to high false positive rates and an inability to catch sophisticated attacks that exploit legitimate processes or user permissions.

Similarly, black box anomaly detection, while promising at the outset, lacks transparency and struggles with a lack of input into cloud native attacks. Millions of such attacks would be needed to create a truly accurate detection model with this approach. These limitations underscore the necessity for a paradigm shift in threat detection methodologies tailored specifically for cloud native environments.

Introducing Behavioral Threat Detection

One of the key pillars of behavioral threat detection is the concept of workload fingerprints that capture the hierarchy of processes, programs, and files of a running workload. Workload fingerprints serve as a baseline for normal behavior within an environment, allowing organizations to detect any deviations or drifts from this baseline. In this approach, the more appropriate usage of AI is not in the detection itself, but in the classification of what has been detected, if it is part of a known attack.

Operationalizing Behavioral Threat Detection

Implementing behavioral threat detection involves several crucial elements:

1. **Baseline Creation**: Establishing a baseline of normal behavior through workload fingerprints, capturing the expected behavior of containerized workloads.
2. **Detecting Anomalies via Drift**: Continuously monitoring and analyzing workload behavior for deviations from the established baseline, leveraging AI-driven analysis to identify potential threats.
3. **Apply Detection to the Software Supply Chain**: Verifying the integrity of software throughout the SDLC by comparing baselined behavior with current behavior, akin to an SBOM for runtime behavior.
4. **Real-time Posture and Context**: Applying real-time context across identity, infrastructure, and workloads to attackers' behavior

Embracing Innovation in Cloud Native Security

The evolution of threat detection and response in cloud native environments demands innovative approaches that can adapt to the dynamic nature of modern applications. Behavioral threat detection, with its focus on understanding patterns of behavior, offers a promising avenue for enhancing security posture and staying ahead of emerging threats. By leveraging workload fingerprinting technology, organizations can take a proactive approach to detection, so that when the next zero day in their cloud environment comes around, they have access to an ultimate source of truth.

About the Author

Jimmy Mesta is the founder and Chief Technology Officer at RAD Security. He is responsible for the technological vision for the RAD Security platform. A veteran security engineering leader focused on building cloud-native security solutions, Jimmy has held various leadership positions with enterprises navigating the growth of cloud services and containerization. Previously, Jimmy was an independent consultant focused on building large-scale cloud security programs, delivering technical security training, producing research and securing some of the largest containerized environments in the world.

You can connect with Jimmy on Linkedin (https://www.linkedin.com/in/jimmymesta/) or by visiting https://rad.security/

Artificial Intelligence in 2024

Major Cyber Threats Powered by AI

By Ed Watal, CEO & Principal, Intellibus

Many have embraced artificial intelligence as a new paradigm, with some even going so far as to call it the “revolution of work.” Unfortunately, people have found ways to abuse artificial intelligence technology, which can cause significant harm to our society.

It is essential to understand that AI is not a threat in and of itself, but rather the users who abuse this technology for their own nefarious gain who are the threat. AI is just like any innovation in history — if there is a way that it can be used for wrong, wrongdoers will find a way to do so.

Perhaps the most praised aspect of artificial intelligence technology is its superior data analysis capabilities. An AI model can analyze larger data sets more quickly and efficiently than a human could. In many industries, this means an ability to reach levels of productivity that were henceforth unattainable.

Still, in the wrong hands, this powerful technology could cause tremendous damage.

How AI is being used to automate cyber attacks

Modern hackers have found ways to leverage AI technology to automate cyber attacks because an AI model can be trained to constantly probe a network for weaknesses, often identifying them before they are even known to network operators. The effects of this are twofold: for one, this significantly increases the number of attacks because attackers can be much more efficient; beyond that, the efficiency of these attacks makes them much more difficult to detect and respond to.

Considering how connected our world is today, the prospect of automated cyber attacks is incredibly frightening. If a hacker targets a high-value target, such as a network powering a supply chain or critical infrastructure, the damage an attack like this could cause could be catastrophic. Everything from shipping routes to traffic lights, air traffic control systems, power grids, telecommunications networks, and financial markets is vulnerable to this type of AI-powered cyber threat.

The abuse of generative AI for scams and fraud

The second potentially harmful capability of artificial intelligence that has taken the world by storm is its ability to synthesize written and audiovisual information from user prompts. This category of AI models, known as generative AI, has been used for several legitimate purposes, including drafting emails, powering customer service chatbots, and more. However, bad actors have still found ways to leverage this technology for their own gain.

One of the most dangerous use cases of AI technology is the improvement of phishing scams. In these schemes, a fraudster attempts to convince a victim to share personal information by impersonating a trusted source, such as a friend, loved one, coworker, boss, or business partner. Although it was once relatively easy to distinguish these fraudulent messages from legitimate ones due to simple mistakes like grammatical errors and inconsistencies in voice, generative AI has allowed scammers to make their messages significantly more convincing. By training a model on a library of materials written by the person they hope to impersonate, scammers can mimic an individual's writing style more accurately and convincingly.

The materials that generative AI can produce extend even beyond writing, as this technology can now also be used to create convincing fraudulent images and audio clips known as deepfakes. Deepfake photos and audio clips have been used for all sorts of nefarious purposes, from reputational damage and blackmail to the spread of misinformation and manipulation of elections or financial markets. With how advanced AI has become, distinguishing between legitimate and fraudulent materials is more difficult than ever.

Fighting fire with fire in AI

Thankfully, many of the tools that wrongdoers use to wreak havoc can also be applied for more positive use cases. For instance, the same models that hackers use to probe networks for vulnerabilities can be leveraged by network operators to identify areas needing improvement on their networks. Additionally,

developers have introduced models that can analyze written and audiovisual materials to determine if they are authentic or AI-generated.

Still, few tools are as potent in the fight against malicious use cases of AI as education. Staying informed about the cyber threats these wrongdoers pose can allow people to be better prepared against their schemes. For example, knowing how to identify phishing scams when dealing with suspicious messages can help people avoid falling victim, and understanding strong cybersecurity practices — including strong password use and access control — can also help protect them from cyberattacks.

Artificial intelligence can and should be a force of positive change in this world, but creating an ecosystem where this powerful innovation can ultimately be used to benefit society requires us to understand and mitigate how it could cause harm. By identifying some of the most common cyber threats that leverage AI technology, we can better understand how to thwart them and allow people to embrace AI for the force of good that it is.

About the Author

Ed Watal is the founder and principal of Intellibus, an INC 5000 Top 100 Software firm based in Reston, Virginia. He regularly serves as a board advisor to the world's largest financial institutions. C-level executives rely on him for IT strategy & architecture due to his business acumen & deep IT knowledge. One of Ed's key projects includes BigParser (an Ethical AI Platform and an A Data Commons for the World). He has also built and sold several Tech & AI startups. Prior to becoming an entrepreneur, he worked in some of the largest global financial institutions, including RBS, Deutsche Bank, and Citigroup. He is the author of numerous articles and one of the defining books on cloud fundamentals called 'Cloud Basics.' Ed has substantial teaching experience and has served as a lecturer for universities globally, including NYU and Stanford. Ed has been featured on Fox News, Information Week, and NewsNation. Ed can be reached online at LinkedIn and at our company website https://www.intellibus.com/.

The Other Lesson from the XZ Utils Supply-Chain Attack

By Thomas Segura, Developer Advocate, GitGuardian

"The best supply chain attack execution ever seen" might sound like yet another hyperbole designed to attract attention, except in the case of the recent XZ Utils case, it was not. Even the most seasoned professionals were left in awe of the sophistication and damage potential the world nearly escaped.

For those who might have missed it, a few weeks ago, a developer discovered through sheer luck—and grit—that a malicious backdoor was present in the widely used open-source compression utility XZ Utils. The backdoor had been intentionally planted in the utility with the intention of gaining virtually unlimited access to most of the servers powering the global infrastructure.

The open-source community's swift response to the recent security incident was nothing short of remarkable. Within mere days of the initial report, the attack was not only identified but fully resolved—all before the compromised version of the tool could spread widely. It's a powerful reminder of the advantages of open source: had this been closed-source code, who knows if the breach would have even been detected, let alone fixed so quickly? Hopefully, this major incident will prompt the industry to develop

more sustainable approaches to open-source software—and, maybe, to make the classic xkcd comic "Dependency" less reflective of the current state of software development.

But from a security standpoint, there's another key takeaway here: in today's world of supply-chain attacks, failing to include GitHub in your attack surface mapping could rapidly become a very costly mistake - especially for companies not actively involved in open-source development themselves.

GitHub: A Double-Edged Sword

GitHub's meteoric rise in popularity has made it an irresistible target for hackers and cybercriminals. With over 300 million public repositories and 100 million users, the platform's vast attack surface provides ample opportunities for malicious actors to exploit. GitHub's widespread adoption across industries, from tech giants to government agencies, means that a single vulnerability or compromised account can have far-reaching consequences.

GitHub was the staging ground for Jia Tan, the (likely fake) profile that patiently built up a history of credibility in preparation for the XZ Utils sabotage. But this is just one example of how threat actors are using the platform to deceive developers: recently, attackers impersonated Dependabot (a bot that checks for outdated dependencies and suggests ready-to-merge changes) to exfiltrate secrets from hundreds of repositories. A study revealed that millions of repositories are potentially vulnerable to "RepoJacking," a supply chain attack that allows malicious actors to gain control over a GitHub namespace by registering a newly available username. The platform's open nature and collaborative features, while essential for fostering innovation, also make it an ideal hunting ground for threat actors. Hackers can easily create accounts, contribute to projects, and even set up malicious repositories that masquerade as legitimate ones.

They can also harvest sensitive data inadvertently exposed on the platform, particularly secrets, of which 12.8 million were exposed just in 2023. This highlights the urgent need for organizations to seriously consider monitoring their GitHub footprint.

The State of Secrets Sprawl

The proliferation of code repositories on GitHub amplifies the risk of sensitive information being exposed, both accidentally and deliberately. In its 2024 edition of the State of Secrets Sprawl, code security company GitGuardian reports that a staggering 12.8 million new secrets occurrences leaked publicly on GitHub in 2023, marking a 28% increase from the previous year. This trend is even more concerning considering the quadrupling of such incidents since 2021.

The report identified over 1 million valid occurrences of Google API secrets, 250,000 Google Cloud secrets, and 140,000 AWS secrets leaked. Many of these leaks concerned enterprise-owned credentials, with the IT sector accounting for nearly 66% of all detected leaks. However, the issue spans various industries, including Education, Science and tech, Retail, Manufacturing, Finance and insurance, highlighting the exposure of many different industries on the code-sharing platform.

One of the report's most alarming findings is that many of these credentials stay valid for a long time, even if the code hosting them disappears from public exposure. A staggering 90% of valid secrets remain active for at least five days after the author is notified, leaving organizations at risk of being vulnerable to what the report calls "zombie leaks." These are lingering credentials that were erased but not invalidated. Because they are still valid and exploitable, they represent an invisible but high-impact vulnerability that could provide attackers with a stealthy way to infiltrate systems.

This critical security gap underscores the urgent need for organizations to implement robust secrets management practices and automate the remediation process to minimize the impact of leaked secrets.

Lessons Learned from the XZ Utils Backdoor Incident

This story underscores a painful but critical truth: that open-source security is not just a concern for IT departments or tech companies—it's a business imperative for all. Today, every organization, regardless of its open-source activity, should prioritize the security of these shared codebases and consider platforms like GitHub integral to their attack surface.

Implementing a comprehensive monitoring and auditing strategy can help organizations mitigate the risk of seeing a key exploited by a malicious actor. For that, they need the ability to identify leaks *outside* of the repositories over which the organization has control, such as personal or open-source repositories. This can be achieved with regular scanning of repositories for exposed secrets, such as API keys, database credentials, and access tokens, which can serve as entry points for attacks.

Investing in automated monitoring and auditing tools can significantly streamline the process and reduce the burden on security teams. These tools can continuously scan repositories, provide real-time alerts, and generate comprehensive reports, enabling organizations to maintain a strong security posture on GitHub.

Moreover, auditing GitHub repositories can uncover hidden threats, such as malicious code injections, backdoors, and supply chain attacks. By thoroughly reviewing code changes, commit histories and contributor activities, organizations can detect suspicious patterns and take swift action to mitigate risks.

However, it is essential to note that monitoring and auditing alone are not sufficient. Organizations must also establish clear policies and procedures for responding to identified risks and vulnerabilities. This includes implementing efficient incident response plans, conducting regular security training for developers, and fostering a culture of security awareness throughout the organization.

By prioritizing proactive monitoring and auditing of GitHub repositories, organizations can effectively reduce their attack surface, protect their valuable assets, and ensure the integrity of their software supply chain. In an era where supply chain attacks are becoming increasingly sophisticated and prevalent, neglecting GitHub security is a risk no organization can afford to take.

About the Author

Thomas Segura, Developer Advocate at GitGuardian has worked as both an analyst and a software engineer consultant for various large French companies. His passion for tech and open-source led him to join GitGuardian as a technical content writer. He now focuses on clarifying the transformative changes that cybersecurity and software are undergoing.

Thomas can be reached online at:

Website: https://www.gitguardian.com/

Twitter: https://twitter.com/GitGuardian

LinkedIn: https://www.linkedin.com/company/gitguardian

How to Best Secure Banking Applications – Top Tips from a Mobile Security Expert

By Krishna Vishnubhotla, VP of Product Strategy at Zimperium

It doesn't take much to guess why cybercriminals increasingly target banking applications including emerging fintech and trading as their prime targets – cybercriminals have and continue to be largely financially-motivated. Recent research found that traditional banking apps accounted for 61% of the apps targeted by 29 specific banking trojans last year, while the other 39% accounted for emerging fintech and trading apps.

What's wrong with traditional security mechanisms employed by these apps? Tools and tactics such as Strong Passwords, Domain-Based Security, One-Time-Passwords (OTP), and Multi-Factor Authentication (MFA) aren't making the cut because they aren't keeping pace with the evasive nature of cybercriminal tactics. Threat actors are aware of where users and organizations spend most of their time and in today's remote reality, that's on mobile devices. So how can banks and financial institutions secure

their banking applications from attacks and thus protect their users' and employees' most sensitive information?

The battle at hand

Before I dive into the solution, let me provide some color to the issue organizations are up against. To address the issue head on, we must have visibility into the scope of the problem.

The Zimperium zLabs team last year discovered 10 new active banking malware families targeting banking applications. The 19 malware families who persisted from 2022 showed new capabilities that pushed them into the category of evasive and, in particular, relentless in their pursuit of financial exploitation. For a malware agent or capability to be characterized as highly evasive means that it shows an ability to sneak past traditional security tooling normally deployed by the majority of organizations. For example, the new trojans leveraged a tactic called Automated Transfer System (ATS Module), which allowed cybercriminals to automate fraud by extracting credentials and account balances, initiating unauthorized transactions, obtaining Multi-Factor Authentication (MFA) tokens, and authorizing fund transfers.

It's also important to consider that users are much more susceptible to mobile-based phishing attacks. As an IT and security leader at a bank or financial institution, you must accept the fact that you no longer hold the reins of employee behavior as tightly as you once did. Where once employees worked largely from managed work devices connected to a central data center, employees are now working remotely from all corners of the earth using a mix of managed and personal devices to transfer data, share documents and communicate. If you provide a banking application for use by either employees or outside users, that is an attractive attack surface for cybercriminals looking to prey on negligent user behavior. And the payoff is lucrative – the breach of financial information has the potential to upend someone's entire life.

Securing precious banking applications

There are four key things that IT and security leaders can do to secure their banking or financial institution. I lay them out below:

- First, **ensure that the application's protection measures match the level of sophistication** of today's threat actors. Your application security team needs advanced code protection techniques that will fight against threat actors who may be able to bypass traditional code protections. These protections should aim to impede the reverse engineering and tampering of mobile applications. Malicious actors have a much harder time dissecting an app when they're confronted with multiple methods of app hardening and anti-tampering. This multi-layered architecture not only deters the creation of targeted malware but also reduces the likelihood of scalable fraud. The goal is to elevate your mobile application security posture to a point where attackers don't see the value and potential gain of attacking

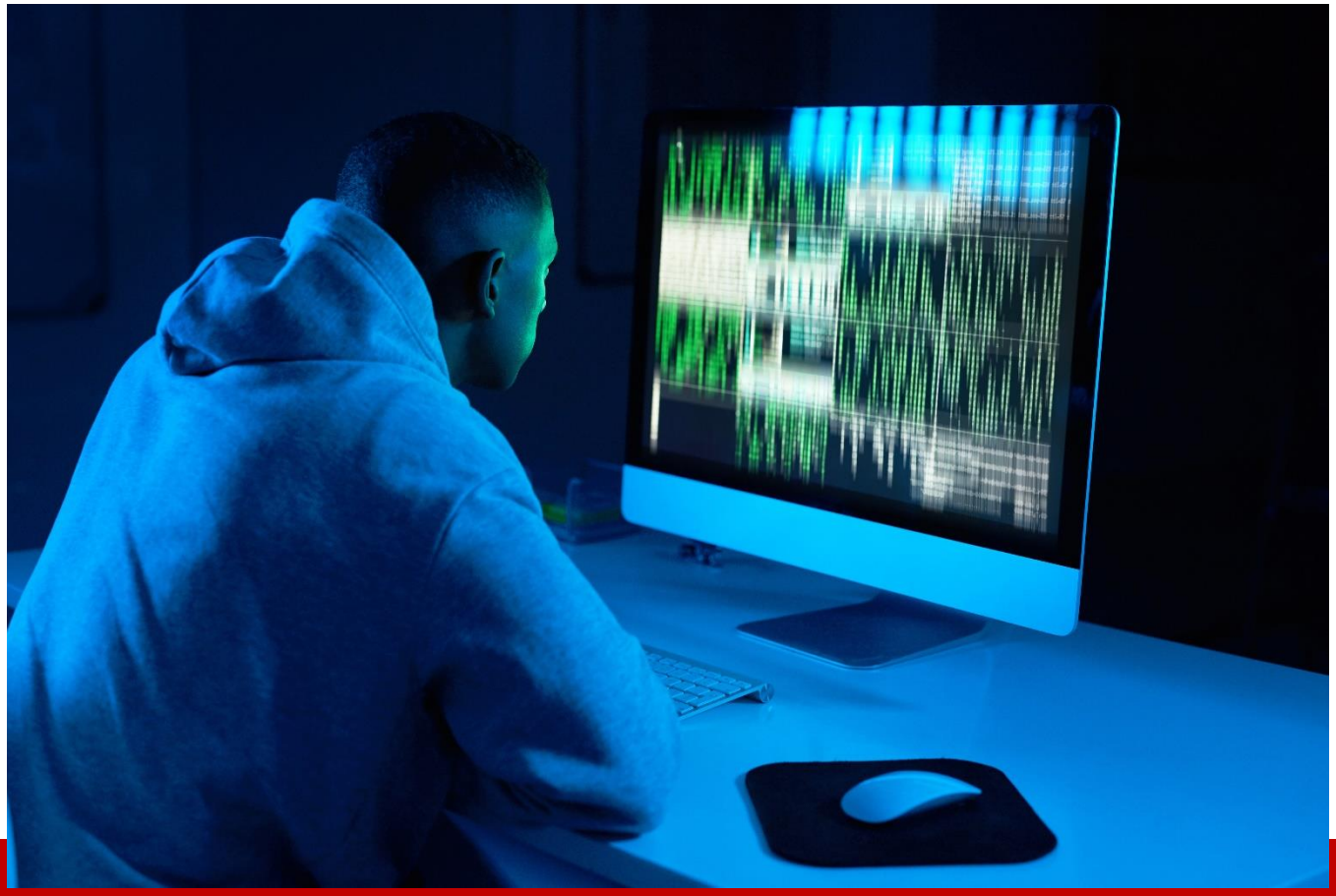
- Second, your teams need to **enable runtime visibility across various threat vectors**, including device, network, application, and phishing. Many security and development teams are operating in the dark, with a limited understanding of the mobile threats targeting their applications on end-user devices in real-time. Zimperium research found that most apps are not compliant with OWASP and MASVS to a great extent. To close this gap, real-time visibility is imperative for active identification and reporting of risks.
- Third, **deploy on-device protection for real-time threat response**. Once you have real-time threat visibility nailed down, it's time for real-time *response.* The whole point of visibility is to respond to threats immediately, not hours or days after. This ability to take action should be autonomous, requiring no dependency on network connectivity or back-end server communication. Of course, the response will depend on the severity and context of the threat, which could include halting the application, changing its behavior dynamically, or redirecting the user to educational material.
- Lastly, it's vital to **invest attention and training towards the consumer**, educating and ensuring that they don't remain a weak point in organizational security. As users of your organization's banking application, it's important they are aware of the danger of too many permissions. Granting accessibility permissions without closely looking at what they are requesting can be risky because these permissions can give apps broad control over a device's functionalities. One of the giveaways that an app is fake is that banking trojans will usually ask for tons of permissions and then will exploit accessibility features to automate transactions, capture sensitive data (such as passwords) or overlay fake login screens on legitimate banking apps.

Attacks targeting mobile applications do share many similarities across industries, but as the security voice for your bank or financial institution, there are nuances in your industry that need to be top of mind. A truly mobile-powered business needs a mobile-first security strategy – and banking institutions that offer applications for their users or employees should remain keen to the tactics of banking trojans and financially-motivated cyber criminals at all times.

About the Author

Krishna Vishnubhotla is a seasoned professional in the SaaS industry, specializing in catalyzing startup growth through adept product and marketing strategies. With a keen focus on mobile application security products, he has a proven track record in defining and executing product visions that drive significant revenue growth. In addition to managing a global customer success portfolio, he established high-value strategic partnerships. His leadership skills extend to spearheading revenue generation efforts, serving a diverse clientele across multiple industries.

Krishna can be reached online at his LinkedIn (https://www.linkedin.com/in/krishna-vishnubhotla/) and at his company website https://www.zimperium.com/.



The Kaiser Data Breach Should Be a Wake-Up Call for Cybersecurity in Healthcare

By Sarah M. Worthy, CEO of DoorSpace

In an alarming revelation, Kaiser Foundation Health Plan reported a data breach impacting over 13 million individuals. For years, there has been an unspoken but critical vulnerability in the healthcare sector's management of digital technologies and personal data. The breach involved online technologies that, unbeknownst to many, transmitted personal information from Kaiser's websites and mobile apps to third-party vendors when accessed by members and patients.

This breach is part of a growing and worrying trend in the healthcare sector, which saw a record 725 large security breaches in 2023, according to The HIPAA Journal. The magnitude of these breaches highlights a systemic issue: a significant gap in cybersecurity knowledge and practices within healthcare organizations.

Understanding the Breach

At the heart of the Kaiser data breach was the improper use of web technologies that facilitated the unintended sharing of sensitive data. These technologies, which often include tracking cookies and other data collection tools, are commonly used on websites to enhance user experience and gather analytics. However, without proper oversight and cybersecurity measures, they can also pose a risk to user privacy by transmitting data to third parties.

This incident reflects a broader misunderstanding of digital fundamentals among healthcare executives. In healthcare, there is an unfortunate and detrimental lack of priority given to cybersecurity. A breach like this happens for one reason only - because healthcare executives and their employees don't understand basic digital concepts such as how web cookies work to collect site visitor data. Healthcare organizations need to take immediate action, because far too many organizations are vulnerable to attacks and breaches despite being in possession of extremely sensitive personal information.

The Cost of Complacency

The consequences of such breaches are not just numbers on a report; they represent millions of individuals whose personal information has been compromised. The implications range from identity theft to financial fraud, all of which can have devastating effects on the affected individuals. These security breaches erode public trust in healthcare institutions, which is something these institutions cannot afford, especially in a sector that deals with sensitive personal health information.

The financial ramifications are also significant, with the industry facing potential losses in the billions due to fines, lawsuits, and remediation costs. Hospital executives and board members need to understand that digital technologies don't simply put their current processes and data into a cloud-based environment and everything else remains 'business as usual.' This shift requires a data-centric focus in operational strategies and a robust understanding of the technologies employed.

Education and Enforcement Moving Forward

To mitigate the risk of future breaches and to safeguard patient data, it is imperative for healthcare organizations to invest in cybersecurity education and training. This initiative must start at the top, with executives leading by example. They need to become proficient in digital literacy, understanding the technologies their organizations employ and the potential risks associated with them.

Further, there should be a mandate for comprehensive cybersecurity training for all employees, tailored to their roles and the specific technologies they use. This training should not be a one-time event but an ongoing process, reflecting the rapidly evolving nature of cyber threats and technologies.

Regulatory bodies need to enforce stricter compliance measures and penalties for breaches, ensuring that healthcare organizations take the necessary precautions to protect patient data. The enforcement of

rigorous standards and practices can serve as a deterrent to complacency and negligence in cybersecurity matters.

The Kaiser data breach is a necessary reminder of the vulnerabilities that exist within the healthcare sector's digital infrastructure. It calls for an immediate reassessment of how healthcare organizations manage and protect personal data. As the industry continues to integrate more digital technologies into its operations, the focus must shift towards building a robust cybersecurity framework that includes education, compliance, and proactive threat mitigation. Only through such comprehensive measures can we hope to protect the integrity of patient data and maintain trust in our healthcare systems.

About the Author

Sarah M. Worthy is the CEO and founder of DoorSpace, a company that is transforming the way healthcare organizations retain and develop talent while solving critical turnover issues in the healthcare industry. Sarah has over 15 years of experience in the B2B technology and healthcare industries. Doorspace's innovative technology "flips the script" on the question from "*what makes people leave?*" to "*what makes people stay?*"

You can find out more about what DoorSpace does at https://doorspaceinc.com/

Looking Past DevOps: AI, ClickOps and Platform Engineering

By Prashanth Nanjundappa, VP, Product Management, Progress

About fifteen years ago, DevOps radically overhauled the world of software engineering. Previously, the development process had been defined by sometimes maddening delays, as development teams waited for operations teams to deploy and run new applications or add a new server. By effectively combining these teams—evenly spreading the responsibility for development and underlying infrastructure—the DevOps paradigm brought a new degree of flexibility to the process. Many of the incredible technological leaps we've seen in the last decade-plus can be attributed to the accelerated development cycles that DevOps facilitates.

But this paradigm brought problems of its own. For one thing, developers had to take on new skill sets, leading to cognitive overload. For another, DevOps practices could lead to a troubling lack of standardization within a given company: three teams might be using entirely different platforms to deliver and run their applications. And then there's the fact that a decade and a half since DevOps became the industry standard, the complexity of the infrastructure underlying new applications has become far more

complex, dependent on countless microservices, each of which DevOps teams must keep in mind as they attempt to iterate new products and generate value for their company.

In recent years, these challenges have led to a wide-scale rethinking of software engineering best practices—a process further accelerated by advancements in machine learning and AI.

The rise of platform engineering is one result of this reevaluation. Effectively, platform engineering standardizes the underlying infrastructure—the cloud platforms, databases and security measures developers need to iterate new digital solutions speedily. Internal developer platforms (IDP) are at the center of this process: scalable, reusable self-service platforms that software developers can use to streamline the development cycle. These IDPs abstract formerly intractable infrastructural complexities, allowing developers to get down to work quickly.

These IDPs are spreading rapidly: according to a recent Port report, 85% of those surveyed indicated they have either already begun implementing IDPs or will do so by 2025. This development dovetails neatly with the rise of ClickOps, rapidly replacing the old code-first approach. In tandem, these automation-heavy tools are helping businesses get more done while reducing levels of employee burnout.

The Rise of 'Click-First' Tools

Typically, a contractor hired to build a house doesn't make the wood themselves; they work with prefabricated materials. The same logic applies to ClickOps. Instead of reinventing the wheel every time, emergent low-code/no-code tools allow software developers to focus more energy on things that add value. They also reduce the barrier of entry for people who have engineering backgrounds. It's no surprise, then, that—according to Fortune Business Insights— between 2021 and 2028, the global low-code development platform market will grow from 14 billion dollars to 95 million dollars.

The benefits here are twofold. First, the automation permitted by ClickOps dramatically shortens development windows: their user-friendly interfaces can reduce development time by up to 90%. Second, simplifying some coding processes allows employees unfamiliar with coding-centric approaches to contribute meaningfully to development processes.

The Role of Generative AI

The rise of platform engineering and ClickOps has been accompanied—and helped along by—rapid advancements in Generative AI (GenAI). Because GenAI can automate tasks, optimize workflows and use pattern detection to suggest potential improvements, it can rapidly speed up development—and turbocharge innovation. A recent McKinsey study shows that software developers can complete important coding tasks (like code documentation, code generation and code refactoring) up to twice as fast by deploying GenAI tools.

These tools aren't merely "useful." Given the unprecedented vast stores of data now generated by even small businesses daily, they're necessary. The most robust IT team cannot analyze this data efficiently

or to keep track of the complex workflows and integrations demanded by contemporary software engineering. In this emerging software paradigm—defined increasingly by ClickOps and platform engineers—AI is an indispensable tool, taming internal sprawl and creating the conditions for developers to do their best work.

Which is to say that AI is not *replacing* developers. Instead, the tools we're discussing here are designed to cut down on busy work and allow developers to apply their ingenuity to more complex, creative tasks. This convergence of human and AI capabilities promises to revolutionize the landscape of DevOps and quicken the pace of overall technological advancement.

About the Author

Prashanth Nanjundappa is VP of Product Management at Progress. He has spent his entire career of over 20 years in the tech world, managing cross-functional high-performance teams, focused on building and launching enterprise and consumer products globally.

In the first 12 years of his career, Prashanth worked as a developer, technical lead and architect for mobile, video-broadcast and OTT, SaaS and PaaS products. Prior to joining Progress, he led the product management teams for high-tech B2B and enterprise products at companies like Cisco and Knowlarity. He has spent time working in Italy, France and South Korea.

Prashanth has an engineering degree in Electronics & Communication from Bangalore University and an MBA from the Indian School of Business (ISB) Hyderabad.

Learn more about Progress here https://www.progress.com/

It Is Time for Smart Cyber Requirements for the Water Sector

By Bob Kolasky, Senior Vice President, Critical Infrastructure, Exiger

Since 2021, the Biden Administration has been consistently talking about the limitations of a purely voluntary approach to cybersecurity for critical infrastructure, and the need for a strategic shift. Among the top priorities for this new focus is the Nation's water sector, which has a long way to go in terms of cybersecurity.

In 2021, the Foundation for Defense of Democracies declared: “The cybersecurity of the water sector is a weak link in U.S. national infrastructure, imperiling health and human safety, national security, and economic stability.”

Despite that recognition, as well as the many efforts by the U.S. Environmental Protection Agency, which serves as the Water and Wastewater Sector Risk Management Agency, and the utilities in the sector itself, that situation remains largely unchanged today. The breadth and scope of the utilities in the water sector, as well as the undercapitalization for infrastructure improvements and underlying technology, means that broad vulnerabilities remain.

This has become a greater concern as continued intelligence reporting – both from the government and from open source intelligence groups, such as Dragos, have found that potential adversaries, including the Chinese government, have a demonstrated interest in developing plans to attack U.S. water infrastructure. Attacks against vulnerable operational technology systems used to operate water and wastewater infrastructure could significantly impact the availability of water, as well as threaten the systems that protect the safety of drinking water. The consequences would likely be amplified by the public fear and uncertainty that would follow.

To veteran cyber defenders, concern about cyber security in the water sector is not new. There has been a longstanding consensus that security controls, culture, capability and capacity are lacking in the sector. With what now looks like an enhanced threat, it is time to reject the existing approach and call for more urgent action in the face of the risk.

We ought to focus on five key areas:

1) Prioritizing progress in cybersecurity on operational technology, the internet of things, and industrial control systems.

2) Ensuring processes are in place to monitor the risk associated with the supply chain of such technologies.

3) Creating a new regulatory framework for water cybersecurity.

4) Utilizing infrastructure investment dollars from rate payments to enhance investments in demonstrable upgrades to underlying digital technology to enable water systems.

5) Enhancing cyber resilience planning so that water delivery can be maintained even in the face of cyber attacks.

Implementing these priorities would result in a strategy that secures the underlying technology that enables the operation of water and wastewater facilities and would push to raise security levels at individual water facilities. It means driving the market to more secure-by-design and secure-by-default technologies.

One change that could be implemented now is the creation of an independent entity to lead the development of cybersecurity requirements, relying on industry expertise and modeled off the electricity sector. The House of Representatives has proposed such an approach in creating a Water Risk and Resilience Organization (WRRO) This would create a more nimble regulatory partnership which could link outcomes, requirements, and controls to threats and vulnerabilities.

In the water sector, like many critical infrastructure industries, cyber security needs to be balanced with business interests and cannot be achieved without investments, which need to be recouped in utility rates. What the proposed Water Risk and Resilience Organization would do is set a defensible standard for the kind of security and technologies that are necessary for more cyber secure water facilities and

mandate that those standards are followed. This would then set market conditions for enabling technologies and help give rate regulators confidence that costs are reasonable and should be part of utility rates.

Another area is the emphasis on resilience. Mandating resilience standards means that water sector organizations will have responsibilities for planning, exercising, and building resilience in case incidents do impact water supply. This makes it less likely that a cyber incident will have a significant cascading impact on communities.

This kind of smart security and resilience regulation is a welcome additive to the purely voluntary approach. It is intended to integrate cyber security and resilience into the "cost of doing business," while relying heavily on private expertise. It is particularly appropriate for the water sector given the current risk environment.

Across many issues, today's cyber and supply chain risk environment requires new strategies and policies – and related structures – to meet the challenges.

The nation's leaders have been clear that the system is "blinking red" in terms of threats. The related changes needed to address them need to be met with appropriate urgency.

About the Author

Bob Kolasky is Senior Vice President of Critical Infrastructure at Exiger, where he directs the development of cutting-edge third party and supply chain risk management technology for the critical infrastructure community. Bob is a widely-recognized expert with over two decades of experience. He's a Nonresident Scholar in the Carnegie Endowment's International Peace's Technology and International Affairs Program, a CSIS Senior Associate, and a Senior Fellow at Auburn University's McCrary Institute. Bob also served the OECD's High-Level Risk Forum Chair. He was the founding Director for CISA's National Risk Management Center, where he co-chaired the Information and Communications Technology Supply Chain Risk Management Task Force. Throughout his career, he's worked for government agencies and contractors, including DHS, GAO, Abrams Learning & Information Systems and Booz Allen Hamilton.

Bob Kolasky can be reached online at LinkedIn and at our company website https://www.exiger.com/

Tightening Water Cybersecurity is Now Imperative as Biden Administration Issues Urgent Warning to State Leaders

By Robin Berthier, Co-Founder & CEO, Network Perception

As the world grapples with escalating cyber threats, the Biden administration has sounded a clarion call to state leaders: bolstering water cybersecurity is not just a priority but an urgent necessity. In March, the Biden administration warned governors that US water and wastewater systems represent an “attractive target” because of their essential nature and frequent lack of “resources and technical capacity to adopt rigorous cybersecurity practices.”

This warning comes at a time when the vulnerabilities of the water sector to cyberattacks have become increasingly apparent, highlighting the need for proactive measures to safeguard one of our most vital resources. In April, American cybersecurity firm and Google subsidiary Mandiant reported that Russian military intelligence hacking operation Sandworm has been linked to a string of recent attackers on water utilities in the United States, including a water system in Texas.

The Biden administration's directive to state leaders emphasizes several key factors driving the imperative for enhanced water cybersecurity

Heightened Threat Landscape: Cyber threats targeting critical infrastructure, including water systems, have become more sophisticated and pervasive in recent years. Malicious actors, ranging from nation-states to criminal organizations, are actively seeking to exploit weaknesses in water infrastructure to disrupt operations, compromise data, and even endanger public health and safety. The administration's warning underscores the gravity of these threats and the need for heightened vigilance

Potential for Catastrophic Consequences: A successful cyberattack on water infrastructure could have catastrophic consequences for communities and regions. Contamination of drinking water supplies, disruption of wastewater treatment processes, or tampering with critical control systems could lead to widespread public health crises, environmental damage, and economic disruption. Recognizing the severity of these risks, the Biden administration is urging state leaders to prioritize water cybersecurity as a matter of national security and public safety.

Interconnectedness with Critical Systems: Water infrastructure is intricately interconnected with other critical systems, including energy, transportation, and telecommunications. A cyberattack on water systems could have cascading effects, disrupting not only water supplies but also impacting essential services across multiple sectors. This interconnectedness underscores the need for a coordinated and comprehensive approach to cybersecurity that addresses not only individual water utilities but also their broader interdependencies within the critical infrastructure landscape.

Leveraging Federal Resources and Expertise: The Biden administration is committed to supporting state and local governments in their efforts to strengthen water cybersecurity. Through initiatives such as the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), federal resources, expertise, and guidance are available to assist state leaders in assessing vulnerabilities, implementing best practices, and responding effectively to cyber threats. By leveraging federal support, state leaders can enhance their cybersecurity posture and better protect water infrastructure against evolving threats.

Building Resilience for the Future: As cyber threats continue to evolve, building resilience within the water sector is paramount. The Biden administration's warning serves as a call to action for state leaders to invest in robust cybersecurity measures, adopt risk-based approaches to threat mitigation, and foster a culture of cybersecurity awareness and preparedness. By taking proactive steps to strengthen water cybersecurity, states can enhance their ability to withstand and recover from cyber incidents, safeguarding water resources for future generations.

In response to the Biden administration's warning, state leaders must prioritize water cybersecurity as a top-tier concern, allocating resources, and attention commensurate with the gravity of the threat. Collaboration among federal, state, and local stakeholders is also essential to effectively address the multifaceted challenges posed by cyber threats to water infrastructure.

At the tactical level, the verification of network segmentation must continue to be prioritized. As attacks on water and wastewater networks grow in size and complexity, network segmentation divides the network into smaller subnetworks, or segments, and controls access between them. This can be accomplished by implementing firewalls, access control lists, and other security measures to control traffic flow between segments. By properly implementing network segmentation principles to protect critical assets, an organization can limit the impact of a cybersecurity breach resulting in continued

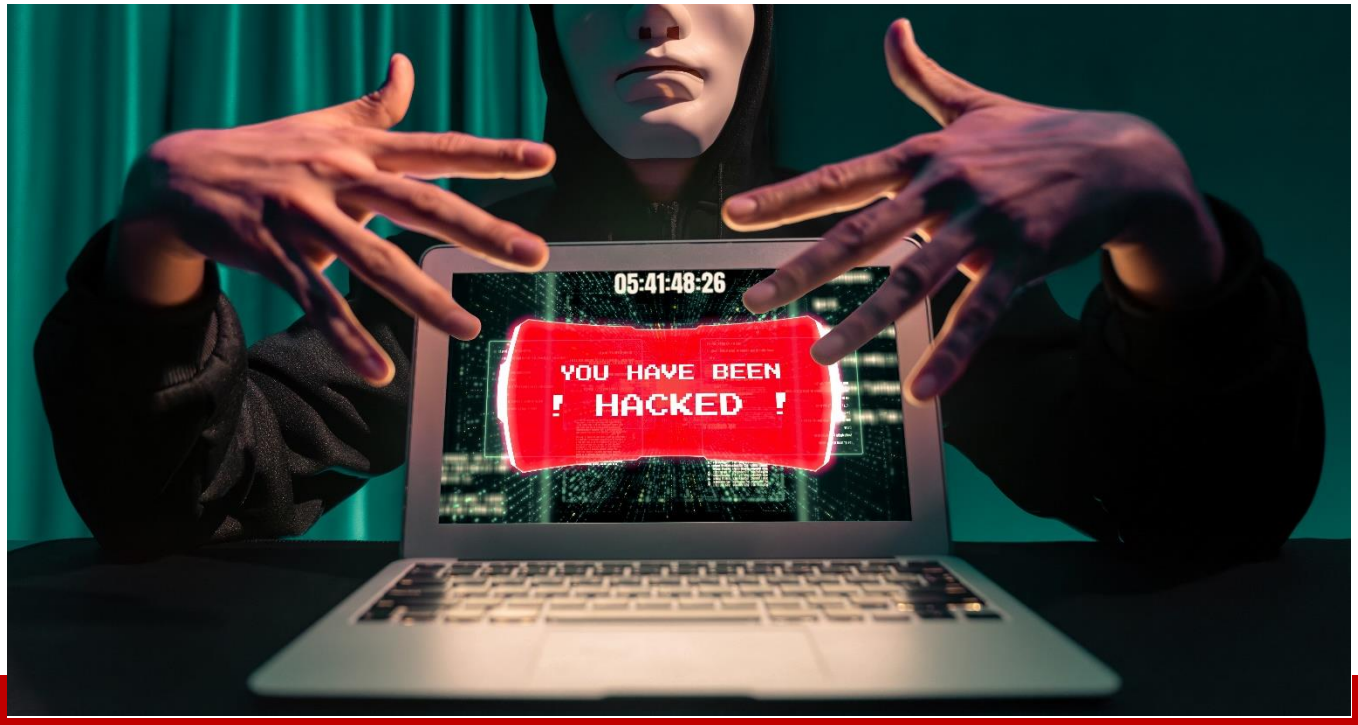
operations and improved recovery times.The benefits of network segmentation are numerous and should be prioritized as a cyber hygiene best practice which assists with building a strong cyber resilient program.

By heeding the administration's call to action and embracing a proactive approach to cybersecurity, state leaders can help secure our water systems against malicious actors and ensure the resilience and reliability of this critical resource.

About the Author

Robin Berthier is Co-Founder and CEO of Network Perception, a startup dedicated to designing and developing highly-usable network modeling solutions. Dr. Berthier has over 15 years of experience in the design and development of network security technologies. He received his PhD in the field of cybersecurity from the University of Maryland College Park and served the Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign as a Research Scientist.

Robin can be reached at rgb@network-perception.com. More information about Network Perception can be found at http://www.network-perception.com



Why Millions of Pcs Aren't Ready for Evolving Cyber Threats

By Achi Lewis, Area VP EMEA for Absolute Security

Ongoing global security threats, underpinned by continuous fears by the White House and NCSC, require an urgent call to bolster security defenses with cyber resilience.

Especially during an era of work-from-anywhere, enterprise organisations worldwide deploy numerous remote and hybrid devices to support their global workforce, presenting a myriad of endpoint security challenges across devices, applications and networks.

Absolute Security's recent Cyber Resilience Risk Index found that a staggering 92 per cent of enterprise PCs are ill-prepared to confront the security challenges accompanying the AI wave. As organisations rush to leverage artificial intelligence, gaps are emerging in the capabilities of both hardware and software, adding yet another layer of complexity for cyber security.

The rising importance of cyber resilience

In response to the ever-evolving threat landscape, the imperative to implement and evolve cyber resilience strategies becomes even more pressing.

Cyber resilience is a paradigm larger and more critical than traditional cyber security, as it not only ensures defenses are working as intended, but also helps organisations withstand and quickly recover from cyber disruptions and attacks.

Gone are the days of merely reacting to breaches, cyber attacks are a case of when, not if, and organisations must work to prevent, react and recover from successful attacks to minimize damage and downtime.

A recent report from the UK National Cyber Security Centre (NCSC) underscored the evolving and significant threat to critical national infrastructure, attributed in part to state-aligned groups. On top of this, the department warned that AI is likely to increasing the global threat of ransomware over the next two years, with AI already causing a rise in frequency.

AI can therefore empower less skilled cyber criminals to conduct more effective attacks, while giving the most dangerous cyber criminals even more firepower.

With a rise in threat level, both in frequency and complexity, there is huge pressure on typically under-resourced security teams to ensure their cyber defenses keep pace. Which is exactly why they need to adopt an approach of cyber resilience.

How AI is complicating security readiness

To run AI applications and processes effectively, including AI-enabled security applications, PCs should be equipped with a minimum of 32GB of RAM and either a stand-alone GPU or an integrated NPU. However, 92% of enterprise PCs have insufficient RAM capacity for AI.

It's no wonder why IDC forecasts that demand for PCs supporting new innovations in AI will surge from 50 million units to 167 million by 2027, an increase of 60%.

This lack of AI readiness can have huge knock-on consequences on security posture.

Significant investment in AI-capable endpoint fleets can often divert budget and resources away from critical IT and security priorities that can leave gaps in security and risk policies – at a time of heightened threat.

Additionally, devices loaded with new software add new security complexities while also impacting performance and security, especially considering endpoint security applications typically fail frequently and many organizations are running behind in critical vulnerability patching.

Ultimately, AI will act, and already is acting, as a double-edged sword when it comes to cyber security. It is introducing more risk as vulnerabilities and AI-enabled threats evolve but can also be adapted into defense technology and procedures by organizations implementing cyber resilience.

When it comes to data security specifically, endpoints that can handle large data sets and language model processing locally can provide an added advantage of storing data on enterprise-owned assets, rather than having to store and process data with third-party cloud hosts. With more localized control over data, organizations can reduce overall risk of data theft and leaks, but only if security and risk controls deployed on the endpoints where data is stored are functioning properly.

Rethinking endpoint protection for enhanced cyber resilience

State-sponsored risks, AI developments and the unpreparedness of enterprise PCs have resulted in traditional strategies for endpoint protection lagging behind the demands of the evolving threat landscape.

To stay ahead of malicious threat actors, it's crucial for organisations to move beyond legacy defense strategies to comprehensive endpoint protection measures that include continuous monitoring, the integration of threat intelligence and the adoption of resilience architecture.

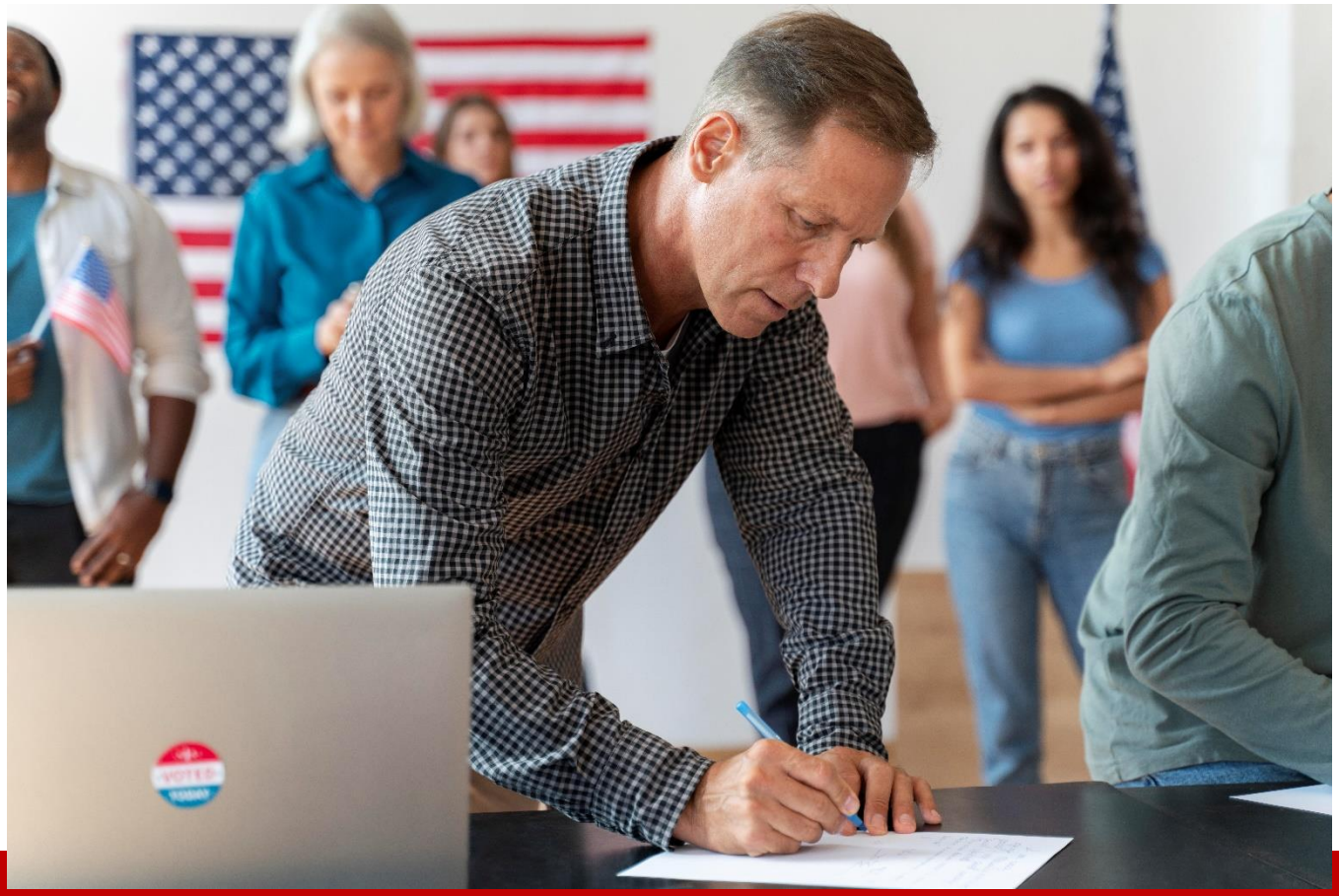
Embracing cyber resilience will enable security teams to maintain visibility over their device fleets and networks, improving their ability to identify potential threats and breaches and swiftly freeze or shut off devices that have been potentially compromised, protecting against major breaches and quickly restoring devices to normal activity with mitigated risk.

By shifting focus towards proactive and adaptive endpoint protection strategies, organisations can bolster their cyber resilience, safeguarding their digital operations against evolving threats and ensuring business continuity.

About the Author

Achi Lewis is the Area VP EMEA of Absolute Security. He is a veteran of the cybersecurity industry with decades of experience in enterprise security, overseeing Absolute's go-to-market strategy in EMEA, establishing relationships with key customers and growing its partner network.

Achi can be reached online at @absolutecorp and at our company website https://www.absolute.com



Cybersecurity Concerns Facing the 2024 U.S. Elections

By Zac Amos, Features Editor, ReHack

Cybersecurity oversights are making infrastructure in the U.S. the most fragile it has been in history. Hackers are constantly developing new strategies to topple critical societal systems, including voting. Election season is here, and experts are analyzing the most prominent threats to design suitable defenses. What does this look like, and do these trends indicate a new future of cybersecure voting practices?

The Election Infrastructure Landscape

Cyberattacks are not uncommon in voting spaces. However, their increasing severity and frequency require more regulatory collaboration and action. Disruptions used to include ransomware, phishing variants and distributed denial-of-service (DDoS) threats.

Hackers still employ these strategies but are evolving in robustness and intricacy. Innovations make it harder for analysts to execute incident response and isolate threats. Novel techniques arise yearly, determined to compromise public trust and dismantle democratic systems.

Historically destructive attacks motivated the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to act. The organization was formed after the Russian-catalyzed decommissioning of voting servers in 2016, which released confidential candidate communications and instigated spear-phishing emails meant to sway results.

The group presented an election strengthening program to the National Association of State Election Directors and the National Association of Secretaries of State to decrease digital risks. It onboarded new hires with election expertise and distributed them nationwide. It will conduct reviews of state-specific election processes and machinery.

AI and Deepfakes

AI phone calls became rampant in New Hampshire as the state approached its primary election window. The robocalls sounded like President Joe Biden and caller IDs falsely showed Kathy Sullivan's name, a former party chair. The impersonation delivered a message to discourage people from voting. Remediation demanded FCC involvement, investigators and multiple cease-and-desist orders to the guilty telecoms company.

The event signified a shift, demonstrating how threat actors will leverage AI capabilities to spread disinformation and dismantle voting rights. Generative AI, deepfakes and chatbots deepen the issue because AI's versatility keeps expanding. For example, hackers may use data poisoning in a machine learning database to fix outputs, leading to falsely informed determinations.

Solving these unprecedented attack variants needs a multipronged plan. New Hampshire prepared by establishing a voter suppression law, but more action is necessary to expound upon AI-specific rules at a federal level. The Biden administration issued an executive order in 2023 to construct policies for dual-use foundation models because of how much data they train and their accelerating development.

CISA recommendations and up-and-coming compliance framework suggestions from organizations like NIST, ISO and OWASP are outlining AI security opportunities applicable to voting systems.

Phishing

Phishing has always been a problem for election officials. The COVID-19 pandemic increased the amount of absentee ballots and online voting registrations, causing the number of digital communications related to elections to skyrocket.

The number of emails, chatbot conversations, instant messages and other forms of communication expands the surface area for hackers to corrupt attachments and pose as reliable individuals. The aforementioned clone voice calls are a form of quishing, or voice phishing.

Actions to prevent this include setting up online forms for gathering data and submitting applications instead of relying exclusively on email. Other initiatives, like the Elections Infrastructure Sharing and Analysis Center (EI-IASC), provide free detection tools for voting centers and city operators. The Election Assistance Commission also recommended these strategies for defending secure voting management systems:

- Employing air-gapping networks
- Using multifactor authentication
- Incorporating physical security measures
- Relying on independent software
- Enhancing voter privacy features
- Encouraging interoperability

Social Engineering

Social manipulation has been a hacking staple for decades but is potent during election season. Cybercriminal outfits bribe, blackmail or persuade election officials, candidates and voters to aid in systemic attacks. These are surefire ways to obtain insider access and information under the radar — even across borders.

Preventing social engineering is a nuanced effort because it often involves mental, emotional and physical motivations unique to individuals with varying degrees of influence. Voting centers and state offices can mitigate social engineering potential by using strict hiring processes with thorough background checks, interviews and references to verify trustworthiness.

Data Breaches

Hackers work endlessly to uncover the many vulnerabilities and backdoors of legacy voting technologies. Websites and voting consoles need updates to withstand new hacking attempts to protect personally identifiable data. Washington, D.C., experienced the vitriol of 600,000 voters in 2023 after a hacking of the city's web host.

Myriad strategies could withstand breach attempts. Filling out workforces with white hat hackers and penetration testers will expediently identify oversights in critical voting infrastructure before cybercriminals make headway. The experts play the role of a threat actor, determining the most valuable opportunity for cybersecurity enhancements.

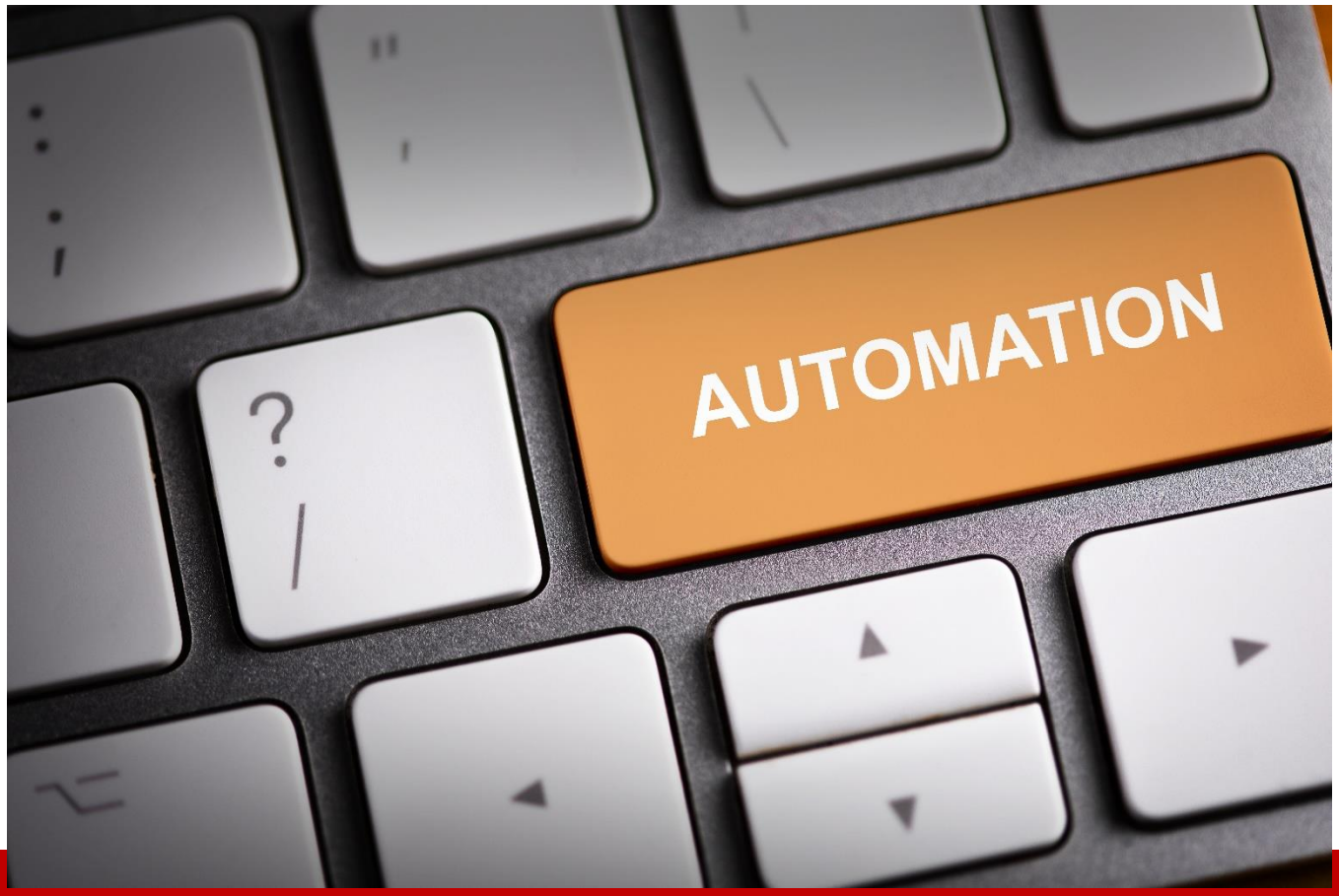
Another solution is immutable storage. Local voting outfits store countless bytes of citizen information, and preserving it in untouchable, uneditable backup hardware could soften a potential breach's devastation.

Protecting Election Security

Cybersecurity professionals must anticipate new attack attempts and styles to prepare adequately. Disruptive technologies like AI will revise antiquated hacking techniques, delivering the stealthiest and most destructive attacks on election infrastructure. Industry professionals and governments must cooperate in developing bipartisan strategies to oppose blows to voting integrity.

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.



Limits of Automation

How Interactive Sandboxing Can Benefit Your Organization

By Vlad Ananin, Technical Writer at Any.Run

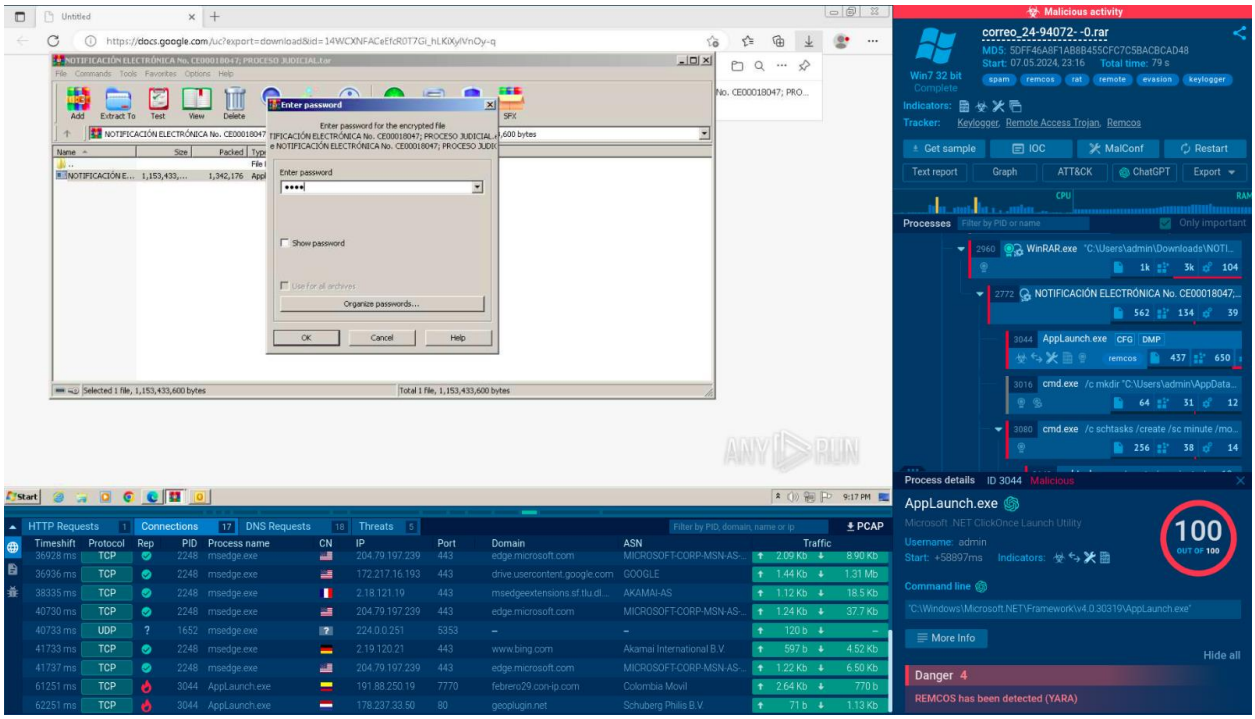
The current rate and complexity of cyber attacks are making it harder than ever for companies to manage their security. In this context, automation provides significant value, alleviating the burden of manual tasks for professionals and improving security operations.

However, some situations still call for human intervention and monitoring. Many of them concern sandboxing. Here are common scenarios where automated sandboxes give way to interactive ones.

What is Interactive Sandboxing?

Interactive sandboxing is a malware analysis approach that combines the speed and scalability of automation with the depth and nuance of manual analysis. Unlike automated sandboxes, which

exclusively rely on predefined scripts and rules to analyze malware, interactive sandboxes enable analysts to manually interact with the malware and manipulate its environment.



Interactive sandbox interface

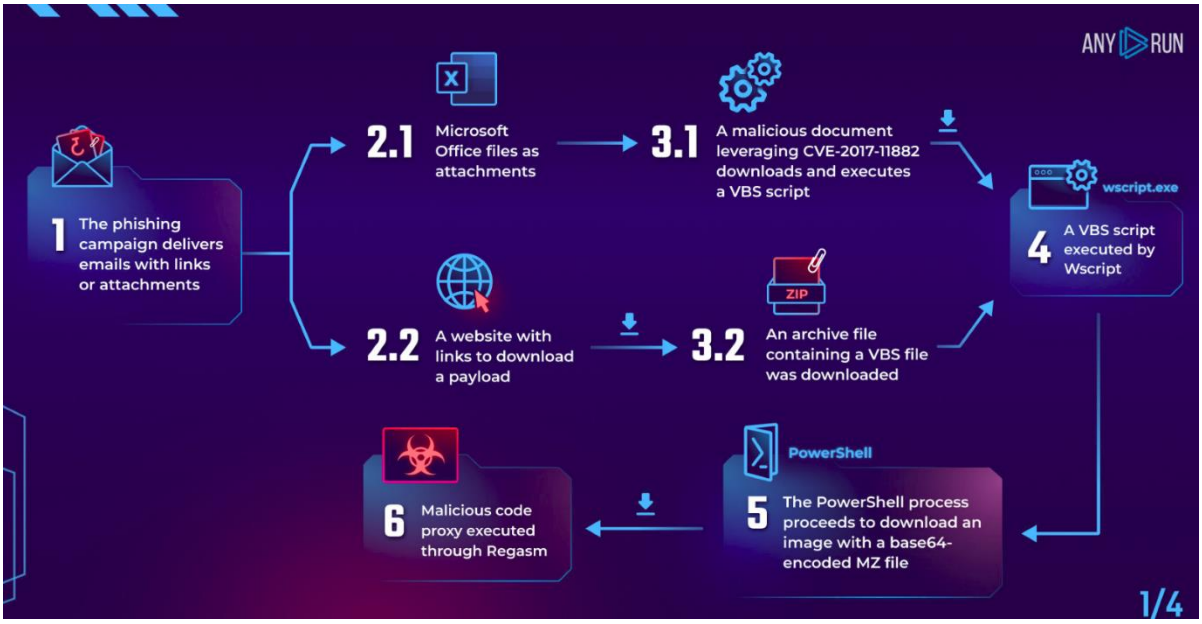
Thanks to interactivity, analysts can perform a wider range of activities that can benefit their investigations. These involve copying from and pasting to the VM, downloading and running additional files, using a web browser, and even rebooting the system. This approach provides a more comprehensive understanding of the malware's behavior, functionality, and intent.

Let’s look at the situations where such an approach proves more effective than the automated one.

Scenario 1: Complex Evasion Techniques

Some malware exhibits behavior that automated sandboxes may struggle to analyze. Such behavior usually concerns the need for human interaction on the part of the user, which is hard to perform in an automated solution. Interactivity allows analysts to engage with the targeted system as they would on an actual computer.

- **Steganography:** Consider the steganography technique, which attackers have employed in many campaigns over the past year. One of the most common implementations of this method involves hiding malicious code inside an image. An interactive sandbox enables analysts to manually extract such content and view its details. Check out this analysis of a stegocampaign, where an image with a base64 encoded executable was used.



Steganography campaign example

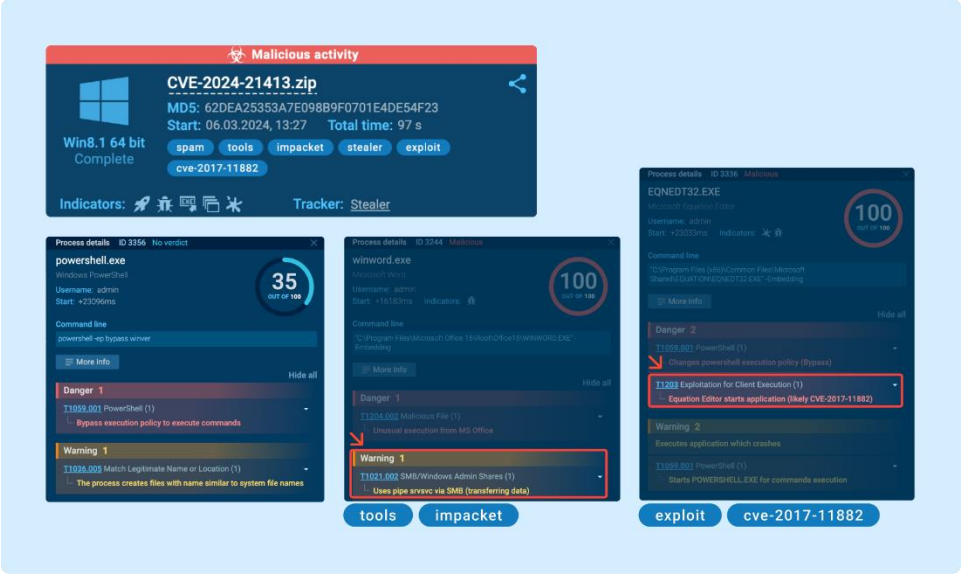
- **CAPTCHAs:** There are also other techniques employed by threat actors that allow them to bypass automated solutions. CAPTCHAs are a prominent example of this, as they have been employed in hundreds of phishing attacks as a simple yet reliable evasion technique. Interactivity enables analysts to easily address this by manually solving the test and proceeding to the next stage of the attack, exposing it entirely.
- **Mouse movement:** Another common sandbox evasion technique involves using mouse movement to trigger malware detonation. While some automated solutions may include mouse emulation mechanics, certain malware can still detect artificial movement. An interactive service can help users overcome this obstacle by providing them with complete control over the virtual machine, making it possible to mimic natural mouse movements and successfully analyze the malware.

Scenario 2: Proof of concept testing

Interactive malware sandboxes are more fitting for proof of concept (PoC) testing compared to automated ones due to their flexibility and customization capabilities. With an interactive sandbox, analysts can manipulate the environment and closely observe the malware's behavior.

This hands-on approach allows analysts to test specific scenarios that may not be covered by automated sandboxes.

Take CVE-2024-21413, also known as MonikerLink, one of the vulnerabilities discovered this year. This flaw can lead to the compromise of an NTLM Hash in Outlook, enabling the remote execution of malicious code without the user's notice.



CVE-2024-21413 sandbox analysis results

An interactive sandbox can greatly benefit professionals who wish to explore the proof of concept of this and other vulnerabilities.

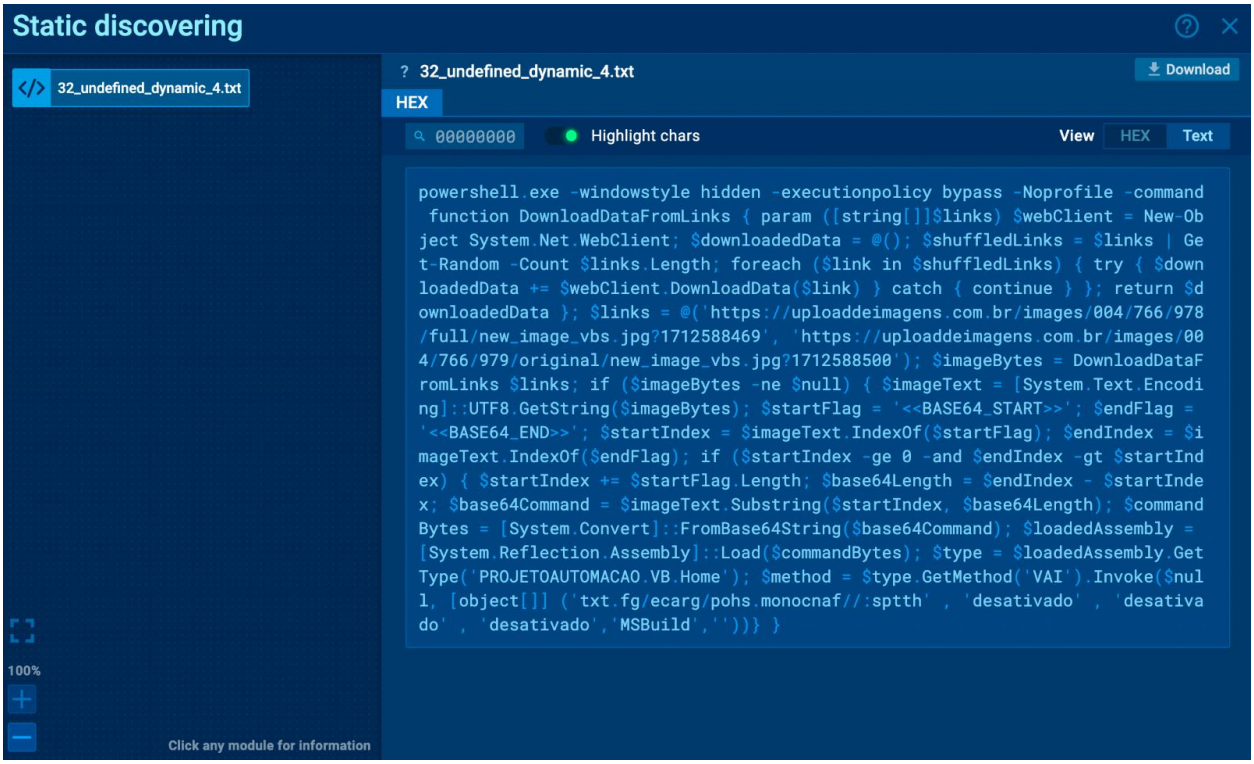
In the case of MonikerLink, they can set up a local VPN network and connect the cloud-based sandbox to it to view the entire attack execution process. Such testing can offer first-hand insights into the vulnerability, which are needed for the training of junior staff and the development of effective detection and mitigation strategies.

Scenario 3: Attack Details

Understanding the details of an attack is crucial for effective response and remediation. However, automated sandboxes may not provide sufficient details about the attack, such as the specific events leading to the infection.

Interactive sandboxes, on the other hand, provide a more exhaustive picture of the attack, highlighting its context and impact.

Script execution that is part of a multi-stage attack is an example of an activity that often lacks details in automated solutions.



Deobfuscated PowerShell script displayed by the sandbox

Interactive sandboxes like ANY.RUN not only detect scripts, including JScript, VBA, and VBScript, executed during the analysis, but also offer a detailed breakdown of their functions, as well as their inputs and outputs. The same goes for PowerShell scripts, found to be the fourth most prevalent TTP in Q1 of 2024. An interactive sandbox simplifies their analysis, presenting a deobfuscated variant of the script for a clearer view of its purpose.

Interactive Malware Analysis with ANY.RUN

ANY.RUN is a cloud-based sandbox designed for interactive analysis. Thanks to the use of VNC technology, users can gain full control over the Windows and Linux VMs and interact with the system directly.

The sandbox on average detects threats in under 40 seconds and extracts indicators of compromise, as well as malware configs of both emerging and persisting malware families.

The service comes equipped with advanced tools for network, registry, and process analysis. It automatically maps all the malicious behavior to the MITRE ATT&CK matrix and generates a downloadable report featuring the findings collected during the analysis.

About the Author

Vlad Ananin is a technical writer at ANY.RUN. With 5 years of experience in covering cybersecurity and technology, he has a passion for making complex concepts accessible to a wider audience and enjoys exploring the latest trends and developments. Vlad can be reached online at the company website https://any.run/

Cyber Resiliency in The Age Of AI: Securing the Digital Perimeter

In the fast-moving age of artificial intelligence (AI), cybersecurity is more important than ever before.

By Tyler Derr, Chief Technology Officer (CTO), Broadridge

In the fast-moving age of artificial intelligence (AI), cybersecurity is more important than ever before. New technologies — especially generative AI (GenAI) — are multiplying the attack surface and accelerating fraud. Today's tech-savvy consumers are well aware of this growing threat to their data, and expect to be protected against it.

Research from Boston Consulting Group has revealed that cybercriminals are 300 times more likely to target financial services firms than any other industry. It's crucial that business leaders in this sector properly address future risks while mitigating them in the present.

AI: Cause and effect

AI is rapidly changing the cyber landscape, making bad actors even more sophisticated, and making it easier for people to become bad actors in the first place.

We know from our own coding practices when we've used AI internally that these tools make already exceptional developers even better.

Unfortunately, the same is true for threat actors. Fraudsters are now able to use GenAI tools to rapidly modify their attacks to help them breach even the most robust cyber defenses.

The good news is that AI can also be harnessed to combat these new threat factors.

Broadridge's 2024 Digital Transformation & Next-Gen Technology Study shows that financial firms are set to boost their investments in cybersecurity by nearly a third (28%) in the next two years. Companies must explore how they can better use the latest AI developments to prevent incidents, and how they can correlate attacks in order to share usable insights across the industry to fight fraud.

Building resiliency at the business level

AI is only part of a much wider story.

Many financial firms are relying heavily on their tech providers for cybersecurity, but they really need to be upskilling their teams at the same time. This could include frequent training sessions covering the pressing topics, such as how to identify and block AI-led phishing attacks, and how to protect personally identifiable information (PII) more effectively.

You shouldn't just be training your cyber department: any role that touches tech is now responsible for cybersecurity. Widespread training can ensure prevention at the point of arrival. This may mean creating a mindset shift for many firms, something that will require a concerted effort.

Even with best-in-class tech solutions and comprehensive training in place, firms still need to plan for what to do if a cyberattack breaks through.

Cybersecurity measures should never be an afterthought, they should be plotted out at the start of all technology projects. Building cyber into your software development lifecycle is another important aspect of building resiliency, which can be supported by enrolling everyone in your cyber defense program.

It's also important to have a proper handle on your partners and any third parties you work with. Make sure you do your due diligence and find out what vendors do to protect themselves. Remember, if they get hit, you will too — and it can irrevocably damage your brand.

Making the case for better data hygiene

True cyber resilience can only be achieved if firms are managing data properly.

Make sure that with any new data, you're only storing what's required from a business perspective. This is the first line of defense, and can help to eliminate unnecessary risk. If there is a leak, and it's related to data you didn't need to store in the first place, the public's perception of the incident will be much worse — as will the regulatory blowback.

Financial firms are of course subject to various disclosure requirements, which are constantly evolving. It's important to be aware of the material non-public information you must disclose. By fully understand the breadth and depth of requirements you can avoid over- or under-disclosure. Again, this can be linked back to only storing data that has a defined business intent.

Prioritizing data privacy certainly pays off for firms. Broadridge's 2024 CX & Communications Consumer Insights report highlighted that consumers are happy to share their data to fuel enhanced customer experiences (CX), but they do expect firms to communicate more clearly about how their data is being used.

Eight in ten (82%) of those surveyed want companies to be more transparent about their plans for user data. Ensuring your company is committed to data security, and being transparent about relevant practices, will also help ease any hesitation from the consumer regarding the inclusion of AI tools.

As frontier technologies such as GenAI disrupt businesses and cyber threats continue to escalate, it's imperative for financial firms to invest in new cybersecurity solutions that are fit for purpose. This investment will mean little if it isn't properly aligned with investment in your own people. By instilling a wider culture of cyber resiliency, you can help your business to navigate this new battlefield.

About the Author

As the Broadridge's Chief Technology Officer (CTO) Tyler Derr is responsible for overseeing Broadridge's global technology teams including software engineering, product delivery, architecture, infrastructure, cybersecurity, and technology operations. He has been at Broadridge for 10 years, firstly as CTO of Broadridge's global technology and operations (GTO) business, and later as chief administrative officer for the same department. Prior to joining Broadridge, Derr worked at OppenheimerFunds. He has also served as the CTO for the global tax business of H&R Block.

The company website is https://www.broadridge.com/

Cybersecurity 101: Understanding the Basics of Online Protection

By Prem Khatri, Vice President of Operations for Chetu, Inc.

In our more and more interconnected world, cybersecurity has turn out to be a paramount challenge for individuals, groups, and corporations of all sizes. With the speedy proliferation of digital technologies and the developing reliance on the internet, the danger of cyber assaults, records breaches, and online vulnerabilities has escalated substantially. Protecting our virtual assets, private records, and online identities has become extra important. This complete manual provides a solid basis for understanding the basics of cybersecurity, permitting you to navigate the net realm with extra self-assurance and attention.

The Evolving Cyber Threat Landscape

The cyber risk landscape is constantly evolving, with new vulnerabilities and attack vectors rising each day. Cybercriminals rent a wide variety of techniques, together with phishing scams, malware infections, allotted denial-of-provider (DDoS) assaults, and complex hacking techniques. Understanding the character of these threats is the first step closer to effective cybersecurity measures.

1. **Malware:** Short for "malicious software program," malware refers to diverse kinds of dangerous packages designed to disrupt, harm, or advantage unauthorized access to pc systems. Common examples consist of viruses, worms, Trojans, and ransomware.
2. **Phishing:** Phishing assaults involve deceiving people into revealing touchy facts, along with login credentials or financial facts, via fraudulent emails, web sites, or messages that appear legitimate.
3. **Social Engineering:** Social engineering exploits human psychology and manipulation techniques to trick individuals into divulging exclusive facts or granting get admission to to systems.
4. **Distributed Denial-of-Service (DDoS) Attacks:** DDoS assaults purpose to crush and disrupt websites or on line offerings by using flooding them with excessive traffic from more than one compromised systems, rendering them unavailable to legitimate users.
5. **Advanced Persistent Threats (APTs):** APTs are sophisticated, targeted cyber attacks carried out with the aid of tremendously professional and properly-resourced threat actors, regularly with the goal of gaining long-time period get entry to to touchy structures or data.

Implementing a Comprehensive Cybersecurity Strategy

Effective cybersecurity requires a multi-layered approach that addresses numerous components of on-line safety. A complete cybersecurity method needs to embody the following key elements:

1. Risk Assessment and Threat Identification

- Conduct normal threat checks to pick out ability vulnerabilities and prioritize mitigation efforts.
- Stay informed approximately rising threats and security advisories from authentic sources.

2. Access Controls and Authentication

- Implement robust authentication mechanisms, which includes multi-factor authentication (MFA), to secure access to important systems and records.
- Manage consumer get entry to privileges based totally at the precept of least privilege, granting only the vital permissions.

3. Data Protection and Encryption

- Employ encryption techniques to guard sensitive records each at rest (saved) and in transit (throughout transmission).
- Implement stable backup and recovery strategies to make certain facts availability and integrity.

4. Network Security and Firewalls

- Configure firewalls and network security solutions to display and control incoming and outgoing visitors.
- Segment networks and put in force secure protocols (e.G., VPNs) for far flung access and information transfers.

5. **Software Updates and Patch Management**
- Regularly update software program, working systems, and applications with the today's safety patches and hotfixes.
- Establish a sturdy patch management method to deal with regarded vulnerabilities right away.

6. **Security Awareness and Training**
- Educate employees and stakeholders on cybersecurity best practices, which include spotting phishing attempts and social engineering procedures.
- Foster a tradition of cybersecurity cognizance in the corporation.

7. **Incident Response and Disaster Recovery**
- Develop and test incident reaction plans to correctly hit upon, include, and get over protection incidents.
- Implement catastrophe restoration techniques to ensure business continuity within the event of a main cyber attack or statistics loss.

Security Compliance Software Development

In modern-day incredibly regulated commercial enterprise environment, making sure compliance with enterprise-specific safety requirements and regulations is critical. Security compliance software development plays a vital role in assisting businesses acquire and keep compliance even as safeguarding their digital property and shielding sensitive facts.

Regulatory Compliance Standards

Various industries have hooked up safety compliance requirements, including PCI-DSS for price card industries, HIPAA for healthcare, and GDPR for statistics privacy.

Compliance software answers can automate the procedure of assessing, monitoring, and reporting compliance with those guidelines.

Risk Management and Governance

Security compliance software program can help organizations in identifying and mitigating risks, implementing robust governance frameworks, and demonstrating adherence to safety nice practices.

Policy Management and Enforcement

These solutions permit groups to define, put in force, and put into effect protection policies consistently across their IT infrastructure, making sure adherence to compliance requirements.

Continuous Monitoring and Auditing

Security compliance software gives continuous monitoring and auditing abilities, permitting groups to song modifications, locate deviations, and generate compliance reports correctly.

Automated Reporting and Documentation

Streamlining the documentation and reporting processes thru computerized answers can extensively reduce the executive burden related to compliance audits and exams.

The Future of Cybersecurity: Emerging Trends and Technologies

As the cyber chance landscape continues to evolve, the field of cybersecurity is swiftly advancing to hold tempo. Several emerging developments and technologies are shaping the future of online safety:

1. **Artificial Intelligence and Machine Learning**
- AI and gadget getting to know techniques are being leveraged for superior threat detection, predictive analytics, and automatic incident reaction.
- These technology can provide real-time analysis of enormous amounts of security information, figuring out patterns and anomalies that may suggest capability threats.

2. **Cloud Security**
- As more organizations migrate to cloud computing environments, cloud security has turn out to be a important cognizance vicinity.
- Cloud carrier companies and security providers are growing specialized solutions to make sure information privateness, get entry to manipulate, and compliance within the cloud.

3. **Zero Trust Security Model**
- The zero agree with security version assumes that no user, device, or utility need to be trusted by way of default, no matter its location or origin.
- This method emphasizes non-stop verification and validation of identities and privileges, improving standard safety posture.

4. **Blockchain and Cybersecurity**
- The decentralized and immutable nature of blockchain generation holds promising packages in regions which includes secure records storage, identification control, and incident tracking.
- Blockchain-based solutions could revolutionize the way we approach cybersecurity and facts integrity.

5. **Cybersecurity Mesh Architecture**
- The cybersecurity mesh architecture is an emerging concept that goals to provide a flexible and scalable method to securing allotted property and sources.
- It entails the integration of diverse safety answers and offerings into a unified and centrally managed platform.

Conclusion

In the virtual age, knowledge the fundamentals of cybersecurity is critical for individuals, corporations, and businesses alike. By recognizing the evolving cyber threat panorama and enforcing a comprehensive cybersecurity approach, we are able to better guard our on-line identities, touchy statistics, and virtual assets.

Cybersecurity is a shared duty that requires a multi-layered technique, encompassing danger assessment, get admission to controls, statistics safety, network security, software updates, safety awareness, and incident reaction planning. Additionally, protection compliance software program development plays a essential role in making sure adherence to industry-precise guidelines and standards, helping corporations preserve a strong safety posture while mitigating compliance risks.

As we look closer to the future, emerging technologies such as synthetic intelligence, blockchain, and the zero trust protection model are poised to revolutionize the cybersecurity landscape. Embracing those improvements even as fostering a lifestyle of continuous learning and adaptability will be key to staying ahead of cyber threats and safeguarding our virtual realm.

Ultimately, cybersecurity is an ongoing adventure that requires vigilance, proactive measures, and a commitment to shielding our online presence. By understanding the basics and staying knowledgeable about the brand new traits and first-rate practices, we can navigate the digital global with confidence and resilience, ensuring a safer and greater secure online experience for all.

About the Author

Prem Khatri is the Vice President of Operations for Chetu, Inc., a global, custom software development company, where he oversees all development projects and technical operations. His primary responsibilities are to lead, track and manage technical teams that create custom software solutions. His background includes software development using C++, Java, and Microsoft technologies. Since joining Chetu in 2008, he has helped the company become an award-winning global presence in the customized software development field. Prior to joining Chetu, Prem worked for Tata Consultancy Services, as well as Blue Star Infotech, and is a graduate of both the University of Mumbai and Savitribai Phule Pune University. Prem is a certified Project Management Professional (PMP).

Prem can be reached at our company website https://www.chetu.com/

Cloud Control: Strategic Insights for Securing Your Digital Infrastructure

By Joe Guerra, M.Ed, CASP+, Professor of Cybersecurity, Hallmark University

When we talk about the cloud, it's not just a buzzword; it's a revolutionary model that has transformed how organizations, from startups to massive corporations and even military institutions, manage and process their information. In this piece, we'll explore the intricate world of cloud platform and infrastructure security, focusing particularly on the strategies behind security controls and the roles of identification, authentication, and authorization (IAM) in cloud environments.

Historical Context and Evolution of Cloud Security Standards

The concept of cloud computing began taking shape in the early 2000s, with Amazon launching its Elastic Compute Cloud in 2006. As organizations began to migrate data and services to the cloud, the necessity for robust security standards became apparent. Initially, cloud security was an extension of IT security;

however, the unique characteristics of the cloud—such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service—prompted the need for more specialized security measures.

Standards and protocols for cloud security have evolved, with significant contributions from organizations like the National Institute of Standards and Technology (NIST). NIST's guidelines on cloud computing have set a benchmark for what security in cloud environments should entail. These guidelines cover everything from general security measures to specific recommendations for public, private, and hybrid clouds.

IAM: The Backbone of Cloud Security

At the heart of cloud security is Identity and Access Management (IAM), which ensures that the right individuals access the right resources at the right times for the right reasons. IAM in the cloud has grown more sophisticated over the years. Techniques and technologies have evolved from basic username and password combinations to more complex systems involving multi-factor authentication (MFA), federated identity management, and single sign-on (SSO).

The military, known for its stringent security requirements, has adopted cloud solutions that incorporate advanced IAM measures. For example, the U.S. Department of Defense (DoD) has implemented cloud strategies that involve strong IAM controls to protect sensitive information while benefiting from the cloud's flexibility and scalability. These controls are meticulously planned and robustly implemented to prevent unauthorized access and data breaches.

In the private sector, companies like Google and Microsoft provide excellent examples of IAM in action. Microsoft's Azure and Google Cloud Platform offer users detailed IAM capabilities, allowing for intricate permission settings and the monitoring of all activities through integrated identity services. These features enable organizations to maintain tight security over their data and applications, even when operating on a global scale.

Planning and Implementing Security Controls in the Cloud

The planning and implementation of security controls in a cloud environment require a strategic approach that aligns with the organization's overall security posture. This process begins with a thorough risk assessment, identifying which assets are most critical and what threats they face in a cloud setting.

Following this, organizations must choose appropriate security controls, tailored to the specific characteristics of the cloud service model they are using (IaaS, PaaS, SaaS). This might involve deploying encryption methods, setting up intrusion detection systems, and implementing strong IAM practices as discussed earlier.

Lastly, continuous monitoring and regular audits are vital. Cloud environments are dynamic, and what might be secure today could be vulnerable tomorrow. Regularly updating the risk assessment and the controls in place ensures ongoing security and compliance with relevant standards.

In conclusion, securing cloud platforms and infrastructure is a complex but critical task. From the military's high-security demands to everyday applications in the private sector, effective planning and implementation of IAM and other security controls are what make the cloud a viable and safe option for handling data in the modern digital world.

A practical example of planning and implementing security controls in a cloud environment can be illustrated by how a healthcare organization transitioned to a cloud-based electronic health records (EHR) system. This move required rigorous security measures due to the sensitive nature of health data and compliance with strict regulations like HIPAA (Health Insurance Portability and Accountability Act).

Scenario: Healthcare Organization Moving to a Cloud-Based EHR System

As the digital landscape evolves, more organizations are embracing cloud technologies to enhance efficiency, scalability, and accessibility of their critical systems. However, this transition also brings forth significant security challenges, particularly when handling sensitive information. A prime example of such a transition is seen in the healthcare industry, where the migration to cloud-based systems must be meticulously planned to protect patient data while complying with stringent regulations like HIPAA.

One illustrative case involves a healthcare organization that decided to move its electronic health records (EHR) system to the cloud. This strategic shift aimed not only to modernize their operations but also to improve data accessibility for healthcare providers and patients alike. Yet, the sensitive nature of the information managed required a comprehensive approach to security. Here's how they approached the planning and implementation of security controls in the cloud, setting a benchmark for best practices in cloud security within the healthcare sector.

Step 1: Risk Assessment

The healthcare organization began by conducting a comprehensive risk assessment focused on the cloud environment. This involved identifying critical data such as patient medical records, billing information, and personal identifiable information (PII). They evaluated potential threats like data breaches, unauthorized access, and data loss due to system failures.

Step 2: Choosing Appropriate Security Controls

Given the sensitive nature of the data involved, the organization opted for a hybrid cloud model to maintain greater control over the most sensitive workloads while still benefiting from the scalability of public cloud resources for less critical data.

Key Security Controls Implemented:

- **Encryption:** All data, both at rest and in transit, was encrypted using advanced encryption standards to protect data confidentiality and integrity.

- **IAM Practices:** They implemented stringent IAM policies that included multi-factor authentication (MFA) for all users, role-based access controls (RBAC) to ensure that personnel could only access data necessary for their job functions, and regular review of access logs and permissions.
- **Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM):** These were deployed to monitor and alert on suspicious activities or potential breaches in real-time.

Step 3: Deployment

The deployment involved close coordination with a cloud services provider that specialized in healthcare data to ensure all configurations were optimized for security and compliance. This included setting up secure VPNs for data transmission, firewalls configured to the strictest settings, and backup systems that could quickly restore data in the event of a loss.

Step 4: Continuous Monitoring and Regular Audits

The dynamic nature of cloud environments and the evolving landscape of cybersecurity threats necessitated ongoing monitoring and regular security audits. The organization used automated tools to continuously scan their cloud infrastructure for vulnerabilities and misconfigurations. Regular penetration testing and compliance audits were scheduled to ensure ongoing adherence to HIPAA and other relevant standards.

Regular Training and Updates: Recognizing the importance of human factors in cybersecurity, the organization also implemented a continuous education program for all employees, focusing on security best practices, recognizing phishing attempts, and safely handling patient data.

Outcome

By meticulously planning and implementing these cloud security controls, the healthcare organization was able to safely migrate to a cloud-based EHR system. This transition not only enhanced their operational efficiency but also maintained the highest levels of data security and regulatory compliance, instilling greater confidence among their patients and stakeholders.

This example showcases how a healthcare organization can address the unique challenges of securing sensitive data in cloud environments through careful planning, tailored security controls, and a commitment to continuous improvement and compliance.

About the Author

Joe Guerra, M.Ed., CASP+, Security+, Network+, Hallmark University

Meet Joe Guerra, a seasoned cybersecurity professor based in the vibrant city of San Antonio, Texas, at the prestigious *Hallmark University*. With a dynamic background as a cyber tool developer for the Department of Defense and the Air Force, Joe brings a wealth of practical knowledge and hands-on experience to the classroom. His journey in cybersecurity education is marked by a diverse teaching portfolio, having imparted wisdom at various esteemed universities across the nation, with a special focus on Texas.

Joe's expertise isn't confined to a single age group or skill level; he has an impressive track record of guiding students ranging from eager high schoolers to career-changing adults. His passion for education shines through in his ability to demystify complex cybersecurity topics, making them accessible and engaging. He thrives on the lightbulb moments of his students as they unravel intricate concepts once thought to be out of reach.

Beyond the realm of cyberspace, Joe is a dedicated father of three, finding joy and balance in family life. His creativity extends to his love for music, often strumming the strings of his guitar, perhaps reflecting on the symphony of cybersecurity's ever-evolving landscape. Joe Guerra stands as a testament to the power of passion, dedication, and the desire to empower through education. www.hallmarkuniversity.edu

Applied Human Threat Management in Cyber Industry

By Milica D. Djekic

The high-tech industry is an extremely emerging environment dealing with the sophisticated and skilled workforce that is recruited to develop an ultimate cutting-edge technology, so far. The majority of things done in that area of the business are highly confidential or if being a contractor with defense or space industries, might be from a national or even global significance especially when there is a word about an international collaboration among law enforcement, military and intelligence communities that do not need an insider risk within their cooperators which could sell some of the projects or professional secrets on the black market or to some of competitors and enemy countries. In other words, it's very important to be confident about the own human resources certainly in a field of cyber industry as those staffing should be managed in a trustworthy, not only skilled manner in order to remain reliable and friendly about their roles within such an employer. On the other hand, the human threat management is a branch of security which copes with pre-, in- and post-employment screenings requiring not just a professionalism, but also some of the background checking, as well as the entire trust management which could be truly correlated with the in-employment screenings, so far. The human threat management is a pretty new concept in security being in use only a couple of years and it is not yet fully developed, but more likely seeks some pioneering effort to get better understanded and implemented into the practice. In addition,

there have always been some competitive intelligence and background checks agencies mainly in a private sector which can sell such sorts of the services to those being interested in and apparently, many advanced economies' governments deal with some standards and legal regulation potentials which are applied to that kind of the well-made marketplace which might be a good source of incomes affecting significantly GDP of the country coping with such security programs.

Depending on how importantly any kind of the employment screenings, background checking and some standards with the laws can impact an overall economy taking into account all independent and objective consequences it is possible to suggest those factors with the total marketplace could be from a vital interest not only for a quality and security in business, but mostly for a wellbeing of the entire social landscape. Indeed, from a strategic point of view, it's very welcome to put into consideration the reasons why someone could invest into such a work as the human threat management should not necessarily rely on a strategy of the fear making everyone believes the safety and security are such drastically needed, but more likely using some soft skills indicating to the governments that if they support such a program they can count on a better economy and greatly developed marketplace which could contribute with the higher GDP and increasing standard to the people. In other words, if the economy is well-developed and the unemployment rate is low, the entire country or, say, the global communities might serve for progress and prosperity across the world, so far. The human threat management as a novel security paradigm has appeared from a need to deal with an accurate and timing finding about the possible risk within some community which means some sort of a theory of the fear has been invoked as those indicators have come from an experience of managing some security challenge and as such empirical results have been very appealing the defense professionals have needed to think hard how to uncover the threat before it becomes too forcing and embarrassing to the rest of the society always getting in mind a counter-intelligence cannot pick up all information from a community, but very likely only those being on the surface and not deeply within someone's personality or, more obviously, some risky routine that person has. From a current perspective, the applied human threat management could mean coping with the risk in the workplace via skill testing, trust management, incident assessment and the other screening programs which should show if there is any reason for worrying truly demanding from the security specialists to in a quite straightforward and practical way, use their experience and expertise in order to create such sorts of the assignments being updated any time a tendency looks for that making a set of the lawful approaches and methodologies which could serve in obtaining a feedback from such a community, so far.

Apparently, if there are some words about the cyber industry, it's very obvious a great majority of those tasks will be done on computers using the highly sophisticated tools and very often the web connectivity which gives some hope those serving in such a field can make a lot of logins leaving a trace in cyberspace and truly uncovering some of their habits and affinities to their employers which in a case of the human threat management, could mean once collecting and analyzing such intelligence it could get feasible to deeply understand all pluses and minuses of those professionals. Also, it's very suitable to think a bit how to do such analytics as user behavior might be a good starting point in getting aware of the potential threat to such an organization suggesting that some sorts of the criteria and wanted goals should be applied in that kind of the human threat management approaches, so far. Moreover, the high-tech industry is also some kind of the critical infrastructure and many using cyber technologies are well-aware that hacker's attacks can occur anytime and anywhere in the world as cyberspace is a very asymmetric surrounding which can make many lessons to everyone as it is not a matter of probability if the cyber

incident could happen, but more likely a causality which must be accepted as inevitable in the everyday life and business not to someone, but mainly to everyone. In total, the role of cyber industry is to assure a cyberspace making such a cutting-edge experience convenient and safe to everyone, but the concern might appear in a sense of the human factor operating in that business which suggests it's undoubtedly good to rely on the experience, as well as some innovative ideas in order to protect all the generations of the humankind have made for a betterment of their own communities and widely the entire global population, so far.

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.

[17] Đekić, M. D., 2022. Static Absorber Modelling. Military Technical Courier

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.

A Closer Look at Recent Changes to New York State Department of Financial Services (NYSDFS) Cybersecurity Regulation

By Christopher Salone, Consulting Manager at FoxPointe Solutions

Most changes to The New York State Department of Financial Services (NYSDFS) Cybersecurity Regulation, 23 NYCRR Part 500, introduced November 2023, have been assigned a compliance date of April 29, 2024. As this deadline fast approaches, the clock is ticking for financial institutions subject to regulation by NYSDFS to make the necessary operational changes to remain compliant and avoid penalties.

This new body of requirements is especially important to thoroughly evaluate ahead of this deadline because it includes critical redefinitions of terms and standards that continue to cause challenges and confusion for financial leaders six months post-introduction of the guidance. Of course, the first step to remaining compliant is to make sure you understand the complex requirements of each guideline.

Below, please find a breakdown of the new expectations included in the regulation that you must adhere to in order to avoid penalties come May.

Expanded Scope

Gone are the days that just banks and insurers have to worry about building a compliant cybersecurity program. This new regulation has expanded the scope of applicability to include financial institutions of any size and third-party service providers.

New terms and classifications have also been introduced that extend regulatory events to new events and entities. For example, cybersecurity “event” and “incident” now have their own categories. A cybersecurity event is any act or attempt, whether successful or not, to disrupt an information system, while an incident is now defined as a cybersecurity event that has occurred at the covered entity, its affiliates, or a third-party service provider that may result in ransomware, material harm, or the need to notify a government body or regulatory agency.

Program and Policy Changes

Financial institutions must now not only conduct independent audits of its cybersecurity program, but also make all documentation of these audits available to the superintendent upon request. Furthermore, these documents must include “relevant and applicable provisions of a cybersecurity program maintained by an affiliate and adopted by the covered entity.”

There is also more oversight now required of corporate cybersecurity policies. Under the new governance, financial institutions must now have their policies approved annually by the senior officer or senior governing body that oversees their compliance, and all procedures must be well-documented in accordance with the approved policy.

For those working to build out their policies, regulations now recommend that all policies include procedures for cybersecurity factors like data retention, end of life management, remote access, and more.

Governance Expectations

New regulations seek to formalize oversight of cybersecurity programs going forward. Financial institutions must now appoint a Chief Information Security Officer (CISO) to present cyber plans, issues, and changes to the Board. The CISO should also be heavily involved in annual reporting, including eradicating any material inadequacies.

Vulnerability Management

Clear and comprehensive policies and procedures regarding vulnerability management must now be documented. These should include preventative procedures like internal and external penetration testing, frequent system scans for vulnerabilities, and timely addressing of those vulnerabilities once identified by security controls planned or in place. These assessments must be updated annually, or whenever there is a change to the business or its utilized technology that impacts the institution's risk.

Data Protections

Speaking of preventative measures, the new regulation is more specific about the kinds of basic security measures required of all financial institutions. For example, access privileges must be strictly enforced, with certain data considered "privileged" based on security risk. Privileged information should be safeguarded with password protection or user access permits that are evaluated and updated annually or when there is a personnel departure.

Multi-factor authentication is another expectation that even covers those technically "exempt" from the new regulations. This standard should be applied to all privileged data, as well as in cases of remote access to the entity's own information systems or that of third-party applications. Encryption is another tool deemed acceptable and recommended by regulatory bodies.

Incident Response

Unfortunately, even the best laid plans can fail, especially in the everchanging digital world we now live in. Due to this, 23 NYCRR Part 500 lays out clear expectations on how entities must prepare and respond to a cybersecurity event or incident. Under the new guidance, financial institutions are required to develop thorough, documented response plans that highlight goals, root cause analysis procedures, and internal processes to follow in the event of a cyber breach. Disaster recovery and business continuity plans should also include data backup procedures and recovery approaches, and once finalized, be distributed to all employees and tested regularly.

After a breach occurs, entities are required to notify the New York State Department of Financial Services within 72 hours – or 24 hours in cases of extortion payments – providing all relevant and requested documentation. Entities, and more specifically, the CISO, must also proactively provide written acknowledgment if they did NOT comply with regulatory requirements regarding the incident, and share a remediation plan.

Monitoring and Training

Human error poses the biggest risk to not only the cybersecurity of an entity, but in the maintenance of compliance. To avoid the consequences of human error, financial institutions must take necessary steps to block malicious content on devices, monitor web traffic, and implement other risk-based controls.

Additionally, cybersecurity training should be conducted annually and during onboarding, and employees should be regularly tested via phishing demonstrations.

These regulatory changes, and many others, have significantly raised the bar for cybersecurity in the financial sector and have demanded increased investments in technology and manpower. If you haven't already, take care in taking the proper action before April 29 to ensure you're well prepared to avoid risks of noncompliance penalties.

About the Author

Christopher Salone, CISA, MBA, CCSFP is a Consulting Manager and Financial Services Practice Leader of FoxPointe Solutions, the Information Risk Management Division of The Bonadio Group. His work focuses on internal and external auditing of information technology and information security practices and controls, providing services to clients across multiple industries, including public and private companies, financial institutions, healthcare organizations, tech companies, and school districts. He conducts audits in accordance with regulatory compliance standards. Christopher can be reached online at csalone@foxpointesolutions.com and at the FoxPointe Solutions website: http://www.foxpointesolutions.com.

The "Non-Trend" of "Full Automation" Workflows in Cybersecurity: A Reality Check

By Oren Koren, CPO & Co-Founder of VERITI

It's no surprise that there's been a shift to automated workflows in the past decade. Initially, automation seemed straightforward: detect malicious activity, eliminate it, and prevent future occurrences. However, this binary approach to cybersecurity soon proved inadequate as the complexity of threats and the environments they target expanded. With the average cost of a data breach costing $4.45 million dollars in 2023, organizations demanded more nuanced solutions, leading to the development of Security Orchestration, Automation, and Response (SOAR) platforms. These systems promised to streamline the incident response process by automating tasks based on various inputs, i.e., logs, events, and alerts, thereby transforming the manual processes of Security Operations Centers (SOCs) and risk teams.

The adoption of SOAR technology by Managed Security Service Providers (MSSPs) and Managed Detection and Response (MDRs) services marked a significant milestone in scaling their offerings. Yet, as the market grew, so did the realization that the promise of complete automation—"let the system handle it"—did not fully align with customer needs. Trust, or rather the lack thereof, in fully automated systems to make critical decisions without human oversight became a glaring issue. But even more so, the question of accountability in the event of a mistake by an automated system loomed large - does the blame fall on the vendor, the security team, or perhaps a developer?

Balancing SOAR in a Dynamic Cyber Landscape

Implementing SOAR solutions presented inherent complexities, largely due to the need for continuous adjustment to meet the vast and evolving cyber challenges organizations face. From new partners and security solutions being added to the organization, not only does the threat landscape expand, but so does the way in which automation responds to these new adjustments. This begs the question then: How do you keep an up-to-date security posture if you don't have full insight into the inner workings of your business environment?

With this skepticism towards full automation, a nuanced market emerged, one that prioritizes security solutions capable of identifying gaps beyond mere log analysis. Modern expectations extend to automation driven by machine learning, offering not just step-by-step playbooks but also the flexibility for customers to engage directly with the remediation process. This approach must be intuitive enough for security analysts to navigate effectively, blending automated efficiency with human judgment.

Rethinking Automation and Building (Human) Trust

The distinction between "automated remediation" and "automatic remediation" has become central to understanding market dynamics. Customers are looking for solutions that provide the scaffolding for automation but leave room for human intervention and decision-making. Furthermore, the demand for open systems, accessible via API for those with the technical prowess, underscores a desire for flexibility and control over automated processes. The key here is adding in some sort of human element because without that automation can't be fully trusted.

The narrative around full automation in cybersecurity has often been romanticized, painting a picture of a self-sufficient, self-correcting system capable of managing security threats without human intervention. However, this overlooks a fundamental aspect of technology adoption: trust. Trust in technology is not a given; it must be earned and maintained through transparency, reliability, and the ability to intervene when necessary. As we move forward, the challenge for vendors and cybersecurity professionals will be to continue refining these technologies, ensuring they are not only effective and efficient but also trustworthy and adaptable to meet the organization's needs and the threats posed.

About the Author

Oren Koren is the Co-Founder and Chief Product Officer of Veriti. Oren brings 19 years of experience in cybersecurity, advanced threat analysis, and product management. Prior to founding Veriti, Oren was a Senior Product Manager at Check Point Software Technologies, where he led AI-based innovations and advanced data analytics projects redefining threat hunting and SIEM applications. Before Check Point, Oren served for 14 years at the prestigious 8200 unit and was responsible for different cybersecurity activities and research. Oren won the Israeli Security Award and 3 MOD awards for cutting-edge innovations in cyber security. Oren can be reached at our company website https://veriti.ai/

AI Can Bridge the Gap of Ineffective MDR Tools

By Orion Cassetto, Head of Marketing, Radiant Security

Last year, nearly one-third of organizations suffered breaches, prompting security professionals to reevaluate the performance of their existing managed detection and response (MDR) solutions, especially as cyberthreats advance in scale, scope and sophistication. A recent survey of 300 IT security experts by Radiant Security showed a widespread dissatisfaction with current MDR tools, and that 60% of respondents are turning to AI tools to ease the pressure caused by ineffective MDR solutions.

AI Becomes More Appealing as MDR Falls Short

A pronounced rise in phishing and social engineering cyberthreats, as well as AI-powered malware, has strained traditional MDR services. The necessity of swift identification and remediation post-breach is paramount for business continuity and resiliency, yet a staggering 44% of MDR users report needing

more than four weeks to address a single incident. This delay grants malicious actors ample opportunity to exploit vulnerabilities, exfiltrate sensitive data, and disrupt operations. The call for redefining security operations is echoed by SOC teams, who seek more innovative approaches as they confront the limitations of MDR.

Furthermore, survey responses have uncovered a potential connection between delayed deployment times and IT dissatisfaction with MDR performance. Half of respondents surveyed experienced a deployment period of four to six months, while an additional 44% faced a seven to twelve-month timeline for total deployment of MDR tools.

How AI Can Support Security Operations

Just over a third, or 34%, of respondents believed their current MDR solutions were incapable of providing a complete picture of their IT environments, a shortcoming that AI and its learning capabilities have the potential to address. Designed to continuously learn and understand, AI can get to know the customer's environment, and offer a more comprehensive view of "normal" activity by examining data sources to evaluate alerts and incidents.

Additionally, AI can provide helpful support to security teams that are understaffed, which is a problem for more than half, or 57% of professionals surveyed. For the 32% of respondents who said their MDR tools escalated beyond the team's capabilities, AI tools can be used to perform extra security checks more effectively than humans, therefore significantly lowering the number of items that are escalated. This can ease the workload for security analysts who are already overwhelmed and cannot spend hours sorting, investigating and responding to all the security alerts they get.

A significant 70% of respondents indicated that time savings for their Security Operations Center (SOC) teams were less than 25% when utilizing current MDR tools. This finding contrasts with the primary objective of outsourcing MDR services, which is to *alleviate* the workload of SOC teams. This is a critical gap in the effectiveness of current MDR tools, leaving organizations in a similar predicament that before they began outsourcing.

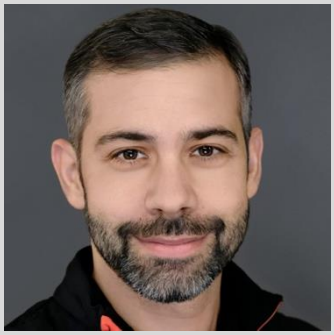
Conversely, the adoption of AI-based security operations presents a promising solution, with the potential to automate 80-90% of Level 1 and Level 2 tasks. By handling triage, investigation, and response tasks at scale, AI-based systems can significantly reduce the workload on SOC teams, thereby aligning with the original intent of outsourcing to MDR services.

Looking Ahead to AI

The incorporation of AI into security procedures presents a game-changing prospect for organizations to bolster their cybersecurity defenses with remarkable efficiency and efficacy, signifying a notable leap forward in combating the escalating complexity of cyber threats. We are in a transformative period in the industry where AI-powered systems are poised to redefine the SOC, facilitating a smooth transition process for organizations and sparking a profound shift in security tactics.

These AI mechanisms are revolutionizing the function of SOC teams by offering an improved contextual comprehension, reducing false positives, and effectively overcoming the constraints associated with conventional MDR tools. By providing much-needed respite and significant time savings, AI enables analysts to concentrate their skills on genuine cyber threats. This critical transition towards AI-led security operations marks a significant milestone in cybersecurity, signaling a future of heightened resilience and efficiency in safeguarding against the continuously changing spectrum of digital threats.

About the Author



Orion Cassetto, the Head of Marketing for Radiant Security. I have over 15 years of experience leading marketing and GTM efforts at successful cyber security companies. Prior to Radiant Security, my roles included VP of Product Marketing at Cycode, Sr. Dir. of PMM at Exabeam, and Dir. of PMM at Imperva.

Orion can be reached online at our company website https://radiantsecurity.ai/company/

The TikTok Ban Spells Trouble for Chinese IoT

What businesses should do today to prepare for likely bans across Chinese tech tomorrow

By Carsten Rhod Gregersen, Founder and CEO of Nabto

It’s happening. Following years of rumors, The United States is moving forward with legislation to ban TikTok. The proposed regulation is about much more than social media and short videos – it's about how a technology company with foreign roots and government links handles sensitive user data.

TikTok is the tip of the Chinese technology iceberg and this is a sign of things to come. As a result, enterprises should prepare as regulators likely move to target hardware, chips, and the Internet of Things (IoT). Let’s explore.

The ban and what it means

This ban has been a long time coming. For example, India banned 60 Chinese apps in 2020, including TikTok, claiming they were transmitting user data back to China. Many, including myself, believed it was a matter of time until similar sentiments gained international traction.

Further, The US has previously banned other Chinese-linked companies for similar concerns. In 2021, Washington cracked down on surveillance equipment from two Chinese companies, Hikvision and Dahua, due to national security and cybersecurity threats. In April, a federal appeals court upheld the ban, ruling that The Federal Communications Commission (FCC) acted within its authority to counteract the national security risk posed by telecommunications equipment accessible to the Chinese government.

While data security is frequently cited as the primary justification behind the ban, the motivations may extend beyond this. They could also reflect the US government's broader desire to diminish China's production capabilities and reduce its economic and technological influence. Thus, the ban likely represents one tactic in Washington's arsenal aimed at China for "flooding global markets with cheap goods."

Now, regardless of whether the Senate moves ahead with the House ban, Washington's protectionist intent is clear. If regulators are concerned about the privacy and security implications of Chinese apps like TikTok, then connected device components and general hardware are next in their crosshairs.

The potential hardware threat

Again, much like TikTok, some view connected devices and hardware from this part of the world as potentially dangerous. This is for three main reasons.

First, data integrity is far from certain. In 2018, China amended its National Intelligence Law, requiring any organization or citizen to support, assist, and cooperate with national intelligence work. What "national intelligence work" means is unclear and, I'd argue, intentionally vague.

Additionally, Beijing acquires "golden shares" in Chinese Big Tech so that government officials are directly involved in these businesses. Again, this raises questions about independence and what's happening on the back end.

Second, nefarious devices can cause big problems. In theory, if granted full permissions within a local network, IoT devices can perform various actions, including monitoring network traffic, initiating distributed denial-of-service attacks, and targeting other connected devices. This is disconcerting from both a business security and national security lens.

Third, the lack of device regulation in this region results in cybersecurity holes. In Europe, there are far-reaching regulations like the General Data Protection Regulation and Cyber Resilience Act. In China, equivalents don't exist. Devices often carry default passwords, always-on cloud settings, and unpatched backdoors. With IoT becoming part and parcel of today's smart home and office, this is just not good enough.

Prepare your business ecosystem now

There's no question that regulators are clamping down on Chinese technology. In fact, one can expect device origin to only grow in importance as the West adopts more protectionist microchip policies (CHIPS and Science Act) and stricter device production rules (Cyber Trust Mark).

This should sound alarm bells for businesses. Overnight bans can translate into overnight bottlenecks if the technology behind your day-to-day operations is suddenly curtailed. The best course of action right now is to evaluate your IoT ecosystem, identify the origins of your software and hardware, and get ahead of any policies that could impact your business.

And, in any case, your information is worth protecting. Chinese devices have a bad reputation for a reason. Despite higher prices, European and American devices often make up for it with data guarantees, tighter controls, and longer lifecycles.

Whatever happens next, staying informed and adaptable is crucial for navigating the changing landscape of global technology governance.

About the Author

Carsten Rhod Gregersen is an IoT expert with more than two decades in software and innovation. Carsten is the CEO and founder of Nabto, the platform providing peer-to-peer communications for connected devices. His areas of expertise span critical domains such as security, cybersecurity, technology regulation, and the impact of IoT. With a proven track record, Carsten lends his strategic insights and operational expertise to various small and medium-sized businesses, serving on multiple boards of directors. In addition, Carsten is a regular contributor to leading media outlets including TechRadar, The New Statesman, Embedded, InfoSecurity Magazine, and many others.

Carsten can be reached online at LinkedIn and his company website https://www.nabto.com/

How to Design a Zero Trust Strategy for Remote Workers

By Federico Charosky, Founder and CEO, Quorum Cyber

The modern workforce expects to work anywhere from any device. To support this approach investment is needed in a broader security program beyond the network. Identity is the new security perimeter as complemented by intelligently managed devices, the applications they run and the data they access.

To answer the question of designing a secure solution for remote workers we need to start by setting some context. First, what is zero trust? This has three pillars which are explained below but can also be encapsulated by the idea that the network carries little trust. The concept of coming to an office to plug into a network point or WiFi to get full access to an organization's resources is swiftly receding. The network has too much of an attack surface, too many hidden doors and is stretched to breaking point (VPN anyone?) to provide a reliable security perimeter. Instead of the network, a zero-trust strategy implies:

1. **Authenticate**. Always and often. Normally user authentication with a username and password, but a lot more in the future.

2. **Time it.** Do you really need Global Admin rights all the time? No user account should have elevated rights, they should all be standard users. And then, as required, the user can elevate their account to obtain more permissions for a fixed time period.
3. **Assume breach.** The question is not will you be attacked, but when. Therefore, invest in defense as well as detection to help limit the blast radius when a breach occurs.

Secondly, for remote workers we assume their network is irrelevant (the network cannot be trusted) and therefore the remote employee can connect using any method such as broadband, mobile, local WiFI and even low-orbit satellites. The key is which device they will use to connect to resources, will the organization allow for any device to access all resources or only corporately issued devices to connect, or a more hybrid approach depending on the data being accessed. They may require a fully patched laptop to access and pay invoices but are allowed to use their personal iPads to access email, for example. Policies can be created to cover countless possible combinations of home owned, corporately owned and corporately issued devices.

The design process will follow four key steps:

1. **Identity**
   The most important factor when creating a remote access strategy. How will your employees authenticate? Traditionally, this has been against on-premises services such as Microsoft Active Directory and more recently cloud-based solutions such as Microsoft Entra ID. Many organizations have already implemented multi-factor authentication (MFA) which cuts down on identity attacks by over 99%, but that is almost now a given. For the future we need to look at removing passwords entirely (the biggest risk to becoming compromised) and look at more modern ways of authenticating, such as Passkeys.
2. **Device**
   Monitor and enforce device health across all the platforms you wish to manage including Bring Your Own Device (BYOD), smartphones and even Internet of Things (IoT) devices.
3. **Applications**
   An application policy can dictate, for example, which email apps are allowed to connect to the email server, which can monitor Shadow IT, enforce Software-as-a-Service (SaaS) usage policies and apply different access permissions depending on the device type.
4. **Data**
   Discover, classify, label, encrypt and restrict access based on a policy. This includes unusual data movement and mass storage events that could indicate data egress via USB storage devices, by ransomware and by various cloud storage services.

The biggest changes for enterprises will be moving to an identity-based perimeter, where nothing is explicitly trusted by default – zero trust! Companies will need to implement a wide-scale data security program to identify and control access to sensitive data, limited to a zero trust least privileged model. To be successful these enterprises will need the right employee skills to design, develop and deploy all elements of the strategy.

About the Author

Federico Charosky is a risk and cyber security expert with a career spanning more than 20 years. He currently leads Quorum Cyber as its Founder and CEO. Quorum Cyber, a UK-based cyber security firm, serves a global clientele across diverse sectors, helping customers win in complex and hostile digital environments. Federico has held several high-ranking positions across the globe. He served as the Head of Security at a Middle East bank, took on the role of Company Director and Head of Consulting at a UK cyber security firm, and acted as a Senior Advisor for numerous prestigious blue chip and FTSE 100 companies. His breadth of experience covers the Americas, Europe, and the Middle East. Federico can be reached online at federico.charosky@quorumcyber.com, https://www.linkedin.com/in/federicocharosky/ and at https://www.quorumcyber.com.

Mastering the Art of Digital Management: Potential Risks and Business Best Practices

By Allison Raley, Partner, Arnall Golden Gregory

Cryptocurrency has opened unprecedented opportunities for businesses to streamline transactions across global markets, revolutionizing the traditional financial landscape. By leveraging blockchain technology, businesses can conduct borderless transactions with greater speed, security, and efficiency. Cryptocurrency eliminates the need for intermediaries, such as banks or payment processors, reducing transaction costs and processing times. Moreover, the decentralized nature of cryptocurrency enables businesses to bypass regulatory hurdles and access markets that were previously inaccessible or prohibitively expensive. With cryptocurrency, businesses can expand their reach, facilitate cross-border trade, and tap into new revenue streams, fostering greater economic growth and global connectivity.

Potential Security Risks

However, as with any new technologies, cryptocurrency is not without its risks. The decentralized and pseudonymous nature of cryptocurrency transactions can create opportunities for illicit activities, such as money laundering, fraud, and cybercrime. Additionally, the volatility of cryptocurrency markets presents inherent risks for businesses as prices are subject to sudden fluctuations and market manipulation. Numerous high-profile hacking incidents resulting in substantial financial losses for businesses and investors have also shown that security vulnerabilities in cryptocurrency exchanges and wallets can pose significant risks. Regulatory uncertainty and compliance challenges further compound the risks associated with cryptocurrency, as businesses must navigate evolving regulatory frameworks and ensure compliance with anti-money laundering (AML) and know your customer (KYC) requirements.

Phishing

The rise of cryptocurrency adoption brings an increased risk of phishing attacks targeting businesses. Phishing, the fraudulent attempt to obtain sensitive information such as usernames, passwords, and financial details, presents a significant threat to businesses operating in the cryptocurrency space. Understanding the nature of these risks and implementing robust security measures is crucial for safeguarding against potential threats.

Phishing attacks against businesses in the cryptocurrency sector can take various forms, ranging from deceptive emails and fake websites to social engineering tactics. These attacks often leverage social engineering techniques to manipulate employees into disclosing sensitive information or transferring funds to fraudulent accounts. For example, attackers may impersonate trusted individuals or organizations, such as cryptocurrency exchanges or wallet providers, to deceive employees into divulging login credentials or authorizing unauthorized transactions.

One common type of phishing attack targeting businesses in the cryptocurrency sector is known as a "fake ICO" or Initial Coin Offering scam. In these scams, attackers create fraudulent websites or social media profiles offering investment opportunities in fake ICOs. Unsuspecting businesses may be lured into investing in these scams, only to discover that the ICO is non-existent or fraudulent, resulting in financial losses and reputational damage.

Another prevalent phishing tactic targeting businesses in the cryptocurrency space is the creation of fake cryptocurrency wallets or exchange platforms. Attackers may create counterfeit websites that closely resemble legitimate cryptocurrency wallets or exchanges, tricking users into entering their login credentials or transferring funds to fraudulent accounts. Once the attackers access the victims' accounts, they can steal funds or manipulate transactions for their gain.

Additional Cybersecurity Concerns

There are additional risks outside of phishing attacks when a business decides to address cryptocurrency on its platform, including:

Payment Fraud: Accepting cryptocurrency payments opens businesses to the risk of payment fraud, where malicious actors attempt to initiate fraudulent transactions or exploit vulnerabilities in payment processing systems to steal funds or digital assets.

Wallet Compromise: Businesses that hold cryptocurrency in digital wallets are susceptible to wallet compromise, where attackers gain unauthorized access to the wallet's private keys or credentials, allowing them to steal or manipulate funds.

Ransomware: Businesses that accept cryptocurrency must be vigilant of ransomware attacks, where attackers encrypt critical data or systems and demand payment in cryptocurrency as ransom for decryption keys.

Compliance Risks: Businesses accepting cryptocurrency must ensure compliance with legal and regulatory requirements governing cryptocurrency transactions, including customer due diligence, transaction monitoring, and reporting suspicious activities to regulatory authorities.

Risk-Mitigation Best Practices

To mitigate the risks associated with phishing attacks and other security issues in the cryptocurrency landscape, businesses must implement robust security measures, conduct thorough due diligence, educate employees about the importance of vigilance and caution, and adhere to best practices for engaging with cryptocurrency.

Some essential strategies for safeguarding your business include:

Employee Training and Awareness: Provide comprehensive training to employees on how to recognize and respond to phishing attempts. Educate them about common phishing tactics and the importance of verifying the authenticity of websites and communications before disclosing sensitive information or authorizing transactions.

Multi-Factor Authentication (MFA): Implement multi-factor authentication for accessing cryptocurrency wallets, exchanges, and other sensitive accounts. MFA adds an extra layer of security by requiring users to provide additional verification, such as a one-time passcode sent to their mobile device, in addition to their login credentials.

Secure Communication Channels: Encourage the use of secure communication channels, such as encrypted email and messaging platforms, to conduct business-related discussions and share sensitive information. Discourage the use of personal email accounts or unsecured messaging apps for work-related communication.

Regular Security Updates and Patch Management: Ensure that all software and applications used by the business, including operating systems, web browsers, and cryptocurrency wallets, are kept up to date with the latest security patches and updates. Regularly review and update security policies and procedures to address emerging threats and vulnerabilities.

Due Diligence and Verification: Before engaging with any cryptocurrency-related platform or investment opportunity, conduct thorough due diligence to verify the legitimacy and reputation of the entity. Beware of unsolicited investment offers or requests for sensitive information and always verify the identity of the sender before responding to any communication.

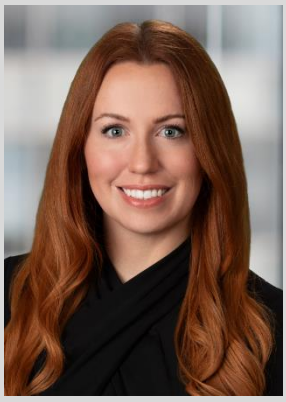
The Importance of Cross-Departmental Training

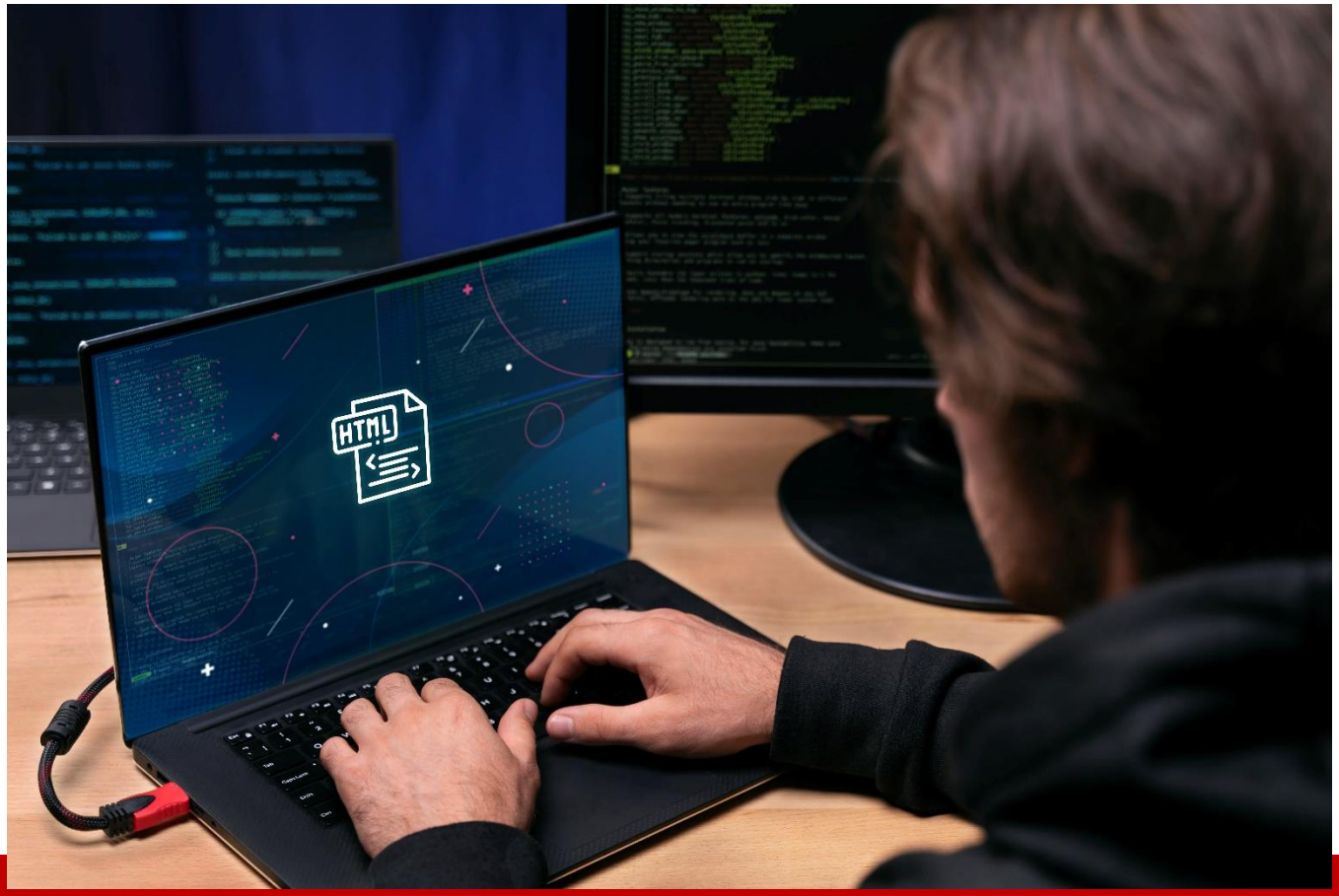
Training multiple people from different departments on managing a company's digital asset account is essential for combating cybersecurity risks associated with employee turnover, which is a common occurrence in organizations. When individuals with specialized knowledge of digital asset management leave, it can create vulnerabilities in the security and integrity of the asset management system. Cross-departmental training on managing digital assets can mitigate the risk of knowledge silos and ensure continuity in asset management processes, as well as allow a diverse team with varied skill sets to bring different perspectives to cybersecurity practices, identify potential vulnerabilities, and implement strong security measures to safeguard against threats. Further, it promotes collaboration and knowledge sharing, empowering employees to collectively address cybersecurity challenges and uphold the integrity of the company's digital assets, even in the face of employee turnover.

By implementing these proactive security measures and fostering a culture of cybersecurity awareness, businesses can effectively mitigate the varying risks present in the cryptocurrency environment.

About the Author

Allison Raley is a partner at Arnall Golden Gregory LLP. She serves as co-chair of the Emerging Technologies industry team and AGG's Women in Tech Law initiative. A former global tech general counsel and chief compliance officer, she serves clients in spaces related to the blockchain ecosystem, AI, payments and fintech, traditional banking and financial services institutions, medical technologies, and industries regulated by the SEC. She can be reached at allison.raley@agg.com.





Combating Cyber-attacks with Threat-Intelligence

Navigate the threat intelligence market's journey through the digital domain and how it integrates to provide a better solution.

By Deboleena Dutta, Junior Content Writer, Research Nester

In today's digitally driven world, organizations face an ever-evolving array of cyber threats. Ranging from sophisticated malware to targeted phishing attacks, the cybersecurity landscape is constantly changing, presenting significant challenges for businesses of all sizes. In response, the demand for effective threat intelligence solutions has never been higher. As per analysis, on average, organizations invest $2.86 million in threat intelligence services.

The threat intelligence domain has emerged as a crucial component of cybersecurity strategies, offering organizations insights into potential threats and vulnerabilities before they can be exploited. But navigating this complex industry can be daunting, with the wide range of vendors offering varying

solutions and services. Here we explore the dynamics of the threat intelligence market, its key players, and the factors driving its growth.

Understanding Threat Intelligence

At its core, threat intelligence involves the collection, analysis, and dissemination of information about potential cybersecurity threats. This information can come from a variety of sources, including security researchers, government agencies, and private sector organizations. Threat intelligence is typically categorized into three main types: strategic, operational, and tactical.

- Strategic intelligence provides high-level insights into long-term trends and emerging threats.
- Operational intelligence focuses on current threats and vulnerabilities relevant to an organization's specific environment.
- Tactical intelligence offers granular details about specific threats, such as indicators of compromise(IOCs) or malware signatures

How is Threat Intelligence Effective?

Threat intelligence provides valuable insights into potential cyber threats, enabling an individual to make informed decisions to protect their organization's assets. By analyzing threat intelligence data, emerging threats can be identified, personnel can understand attack vectors, and prioritize security measures effectively. This proactive approach helps strengthen the organization's security posture and mitigate risks before they escalate into major incidents.

Threat Intelligence Domain - Applications

The applications for threat intelligence are diverse and encompass a wide range of use cases across various industries. Some of the key applications present in the threat intelligence market are:

- Proactive Threat Detection - Organizations are able to recognize and foresee possible cyber threats before they materialize into extensive attacks thanks to threat intelligence. Organizations can reduce the risk of data breaches and system compromises by proactively detecting and neutralizing threats in their early stages through continuous monitoring for indicators of compromise (IOCs) and developing threat trends.

- Fraud Detection and Prevention - Threat intelligence is also helpful in identifying and stopping fraudulent activity, including identity theft, financial fraud, and phishing schemes. Organizations can spot suspicious activity suggestive of fraud and take preventative action to lessen the risk of monetary losses and reputational harm by examining trends and anomalies in user behavior, transaction data, and communication channels.

- Incident Response and Mitigation - Threat intelligence offers important insights that speed up incident reaction and mitigation actions in the case of a security incident or breach. Organizations can rapidly evaluate the extent and gravity of an assault, pinpoint the tactics, methods, and procedures (TTPs) employed by adversaries, and execute focused remedial actions to eliminate the threat by integrating incident data with threat intelligence feeds.

- Regulatory Compliance - An organization's ability to comply with industry rules and data protection legislation is greatly aided by threat intelligence. Organizations can meet the strict criteria of industry standards bodies and regulatory agencies by demonstrating due diligence in recognizing and mitigating cyber threats through the integration of threat information into their security frameworks.

The Market Landscape

The Industry for threat intelligence is expected to reach USD 55 billion by the end of 2035, and it continues to grow at a constant 16% compound annual growth rate over the past several years. The threat intelligence industry was estimated at $11 billion by 2022. To prevent a growing number of cyber attacks on all levels, threat intelligence is mainly used. It was estimated that each day around 2,220 cyberattacks happen, equating to over 800,000 attacks each year.

In view of the increasing cyber conflict among attackers and defenders, most organizations focus on the integration of threat intelligence and other cybersecurity measures. Consequently, enterprises are encouraged to make quicker and more effective security options and to work against breaches, given the deployment of threat intelligence.

Driving Forces Behind Market Growth

- Growing penetration of Internet Services – Global digitization has led to the development of Internet services which increases the chance of cyber threats. Thus, secure control systems such as threat intelligence are being deployed in the industries. As of January 2023, there were almost 5 billion internet users worldwide.
- Surging Data Breaches & Cloud Threats – The emergence of digital technologies has increased cloud threats and data breaches which subsequently require threat intelligence for the fight against data theft. In 45% of cases, the breach is cloud-based. A recent poll found that 27% of enterprises had encountered a public cloud security event, an increase of 10% from the previous year, and that 80% of businesses had experienced at least one cloud security incident in the year,2023.
- Accretion of Industrial systems & digital technologies – The rapidly evolving technological landscape is causing a global transition in a number of industry verticals. Industrial transformation and the development of digital technologies have accelerated as a result. As a result, industrial systems and digital technologies have combined to form a unified ecosystem. This presents profitable potential for IIoT and M2M communication technology.

Additionally, the use of digital technologies has expanded even more as a result of COVID-19. According to projections, the global expenditure on digital transformation is expected to reach around USD 3.4 trillion by 2026. Additionally, The World Economic Forum estimates that by 2025, digital transformation will bring $100 trillion to the global economy. Furthermore, it is poised that by 2025, platform-driven interactions will facilitate almost two-thirds of the $100 trillion in value that digitization holds.

Segmentation Analysis:

Component	• Solutions • Services	The solution segment holds the largest market share. With realtime insight from threat intelligence solutions, operational security teams can save time and increase efficiency, thus driving segment growth.
Type	• Strategic • Tactical • Operational	The operational segment held the largest industry share. This is due to an increase in the demand for information about specific incoming attacks by hackers.
Deployment	• Cloud • On-premise	The cloud segment is analyzed to garner the highest market value. In the face of increasing cyber threats, cloud services play an important role. This has led to a tremendous increase in the use of cloud threat intelligence tools over the past several years.
Organization Size	• SMEs • Large Enterprise	The SMEs segment is slated to have great opportunities. Globally, SMEs become targets for new types of cyber attacks and thus are in favour

		of using threat intelligence services. For instance, in 2021, 61% were targets for cyberattacks.
End-User	• BFSI • Government & Defense • Education • IT & Telecom • Manufacturing • Healthcare • Energy & Utilities • Retail	The IT & Telecom segment is estimated to gain significant market share, owing to the trend of digitalization. Also, the adoption of technologies such as a 5G and cloud services in the IT sector brings the need to use threat intelligence.

Regional Analysis

The regional analysis for the threat intelligence market typically highlights key trends and factors affecting the sector's growth in different geopraphical areas. Here's a breakdown of some common regions and their significance:

- North America:
  - Leading market due to the presence of major cybersecurity companies and early adoption of advanced security technologies.
  - Strong government initiatives to combat cyber threats contribute to the market's growth.
  - High investment in research and development activities driving innovation in threat intelligence solutions.
- Europe:
  - Growing concern over cybersecurity threats fuels the market demand. For instance, Germany largely suffered from ransomware attacks (52%) and denial-of-service attacks(43%).
  - Stringent regulations such as GDPR(General Data Protection Regulation) drive organizations to invest in threat intelligence solutions for compliance.
  - Increasing collaborations between government and private sector entities to enhance cyber resilience.
- Asia Pacific :
  - Rapid digitization and expanding IT infrastructure lead to increased vulnerability to cyber threats, driving demand for threat intelligence solutions.
  - Growing awareness among enterprises about the importance of cybersecurity amplifies market growth.

- Rising investments in cybersecurity by governments and organizations to address evolving threats.

Key Players

- IBM Corporation
- Check Point Software Technologies Ltd
- CrowdStrike, Inc.
- AO Kaspersky Lab
- Anomali, Inc.

Latest Innovations

- Oct 2023- Aiming to expedite security response timelines for clients, IBM revealed the next evolution of its managed detection and response service offerings with new AI technologies. These technologies include the capacity to autonomously escalate or close up to 85% of alerts. The brand-new Threat Detection and Response Services (TDR) offer automatic security alarm remediation, monitoring, and investigation around the clock for all pertinent technologies in clients' hybrid cloud environments.
- Feb 2024 - A leading provider of cloud-delivered, AI-powered cyber security platforms, Check Point® Software Technologies Ltd., is pleased to present the Check Point Quantum Force series, an inventive range of ten high-performance firewalls built to meet and surpass the demanding security requirements of enterprise data centers, network perimeters, campuses, and businesses of all sizes.
- Sept 2023- In a staggered rollout, Symantec, a division of Broadcom Inc., and Google Cloud will integrate generative artificial intelligence (gen AI) into the Symantec Security platform, offering customers a major technological advantage in identifying, comprehending, and mitigating sophisticated cyberattacks.
- March 2024 - A strategic alliance between CrowdStrike and Rubrik was announced to accelerate data security transformation and prevent compromises of vital data. Organizations can quickly identify, look into, and stop attacks targeting sensitive data by combining the industry-leading AI-native CrowdStrike Falcon® XDR platform with a comprehensive, data-centric attack context from the Rubrik Security Cloud.

Conclusion

One of the most crucial elements of the rapidly expanding digital world is threat intelligence. As far as cyber-attacks are concerned, threat intelligence allows organizations to act proactively instead of reactively. It is not possible to protect successfully against cyber attacks unless we understand security vulnerabilities, threat indicators, and how threats are made. Threat intelligence can assist lower the risk

of cyberattacks, strengthen security posture, and facilitate the team's ability to respond to situations more skillfully as cyber attackers become more sophisticated.

Source:

https://www.researchnester.com/reports/threat-intelligence-market/5138

About the Author

Deboleena Dutta currently works as a Junior Content writer for Research Nester. A Biotech engineer by profession, she ventured into the field of writing to find her inner passion. Having had experience for 11 months, she enhanced her skills in business writing, research, and editing. Being a bibliophile has helped her play with words in her profession as a content writer. Her hobbies are listening to music, dancing, and painting.

Deboleena Dutta can be reached at https://www.researchnester.com/

Emerging Technology Review and Needs

By Milica D. Djekic

The progress distribution is a slow and time-consuming process that normally might take decades and sometimes centuries in order to deliver a betterment for many to the majority across the globe. The new millennium has started with a plenty of great scientific ideas and proposals, but also it has given a highly appealing lesson to the humankind warning the majority of the global population how it appears living and working in an unsafe and pretty unsecure world which has made everyone being dependable on speculating reliable and less trustworthy technology, so far. In other words, the main challenge with this novel time is how to remain cyber safe in an environment of the always evolving threat which has a capacity to significantly impact critical infrastructure and consequently, hurt people, processes and technologies. Apparently, high-tech security has become an imperative in protecting the entire nations and their countries and the fact is such a marketplace has turned into well-developed ecosystem which

can offer a lot, but cannot provide an absolute assurance as those using such solutions and services will never be remained in the peace for a reason some risk must be chronically present concerning gatekeepers in their mission to even reduce that unwanted pillar, so far. On the other hand, the fourth industrial revolution has brought a heap of new technological systems such as an artificial intelligence (AI) being in its weak phase of the deployment and many recognized researchers believe a strong age of the AI yet needs to come leaving a lot of places to those who are looking for applied AI outcomes. The point is scientists, engineers and innovators of nowadays must serve hard in order to make a marriage between extremely demanding cyber defense usages and truly promising AI perspectives as those two areas should live in harmony, synergy and collaboration with one another, because those both disciplines of science and practice are still on their road to get much more developed and deeply applied in a very dynamic and complicated surrounding, so far. The purpose of this article is to offer some initial suggestions, letting a potential for much deeper research, which should open up a true scientific, professional and expert's discussion about the pluses and minuses of those quite close, but yet not completely explored areas of technology.

The low-voltage electronics systems have noticed their boom after the World War 2 bringing with themselves some practical applications of the binary algebra which have led to the digitalization as it is well-known today. The digital technologies are widespread worldwide nowadays and many have mastered how to design and produce some of such technical solutions which makes those endeavors being suitable and available to the majority of the international population, so far. In other words, when an offering is huge a pricing should be lower as the multinational giants, as well as some startups yet have an interest to overwhelm the marketplace with their products and services as getting something accessible to many means being better competitive then the rest of the competitors and providing a plenty of qualitative and still cost-effective outcomes. Indeed, the quality and price can go together as if the marketplace is big such a condition might cover all the offering's expanses and yet count on some profit which can be, say, 2 or 3 percentages which is in case of ungreedy business more than sufficient which suggests it is worth of putting such a time and effort into that mission. Especially, it is interesting to mention that the majority of the hardware and electronic devices in a digital technology arena are made from semiconductors such as silicon which can be isolated from a sand being a building block for making something cheap and yet functional which might dramatically impact a curve of the optimal solution suggesting that the optimal product or service can provide a high functionality for a very reasonable price. It seems investing into research of the semiconductors technologies could be an extremely return-of-investment (ROI) process as it is truly needed to make some comparing of the industry being available at the present and the industry coming from such an inexpensive and anywhere reaching resource as the silicon is, so far. Further, from a strategic perspective, many world's corporations and business actors have a deep influence on their governments and the other international organizations seeking from them to push some of their interests through a legal regulation which is well-accepted from a point of view of the national, regional and even global economies. Apparently, many could be lured to invest into such activities as their ROI could be good and to such an experience, the entire distribution of the progress at the global scale could be accelerated requiring less time for betterment and prosperity come to the developing societies and even the most undeveloped parts of the world, so far. In addition, the humankind could significantly progress as a civilization dealing with the equally good opportunities mainly to all members of its family.

No technology is safe from a security risk even being physical and, in this case, virtual being strongly correlated with the current information-communication technologies (ICT) that are mostly something many can see as a cyberspace, so far. With the appealingly high demand for a cyber security in the majority of progressive countries and initially led by the United States there has appeared a totally new branch of the commerce being a cyber industry which in order to acquire the biggest possible marketplace sometimes has used a language of the fear trying to aware a business sector to invest into ICT defense, but after realizing the results to that strategy are poor switched to an approach being much closer to the business people as it is always challenging to make players pay more if they happily can live without such offerings and stay with a more money in their pockets. That was an attitude yesterday, but nowadays many have become convinced that under arising threat from a terrorism mostly, as well as the other asymmetric challenges the cyber security has turned in a requirement many will appreciate and their governments once getting confident about the very feasible consequences to the critical infrastructure have approved such national strategies and legal regulations, so far. It's fully difficult adopting such an approach as the ongoing lessons from a modern history are quite unhandy and no one would want them ever happen to anyone again, so that's why such a need has been recognized and maybe that is not a completely global trend as in some parts of the world it's yet too costy investing funds into those technological landscapes as in the low-level economy countries the money is not an only concern, but more likely a skill shortage is enormously large and those guys simply cannot resolve any of such complicated and complex tasks, so far. In other words, cyber defense looks for an international collaboration as the domestic, regional and global policing organizations must cope with both – human and technological resources to tackle a cybercrime. The experience suggests that the majority of those asymmetric threats are deeply linked with the transnational organized crime and terrorism and it is only a matter of time when someone can drastically attack from the cyberspace and affect the lives of many in a truly negative connotation, so far. The fact is any technological weapon must have its adequate counter-weapon which might respond to an always arising threat which in the best-case scenario, should be prevented to even occur which is an extremely hard problem to those who are not having a technical capacity and if they just have, they cannot count on people who could be enough skilled to even use that. Next, in the modern time, the information travels in a sub-second period of time and even if some defense agencies are technologically equipped, they need a plenty of time to train their human capacities to get vetting about their highly demanding tasks being assigned to them in order to let them provide the best possible response to the crime and literally stay at least a step ahead of the bad guys.

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.

[17] Đekić, M. D., 2022. Static Absorber Modelling. Military Technical Courier

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.

The Challenge of Combatting Threats Against Autonomous Vehicles

By Joseph Hladik, Cyber Group Lead, Neya Systems

From perception and sensing to mapping and localization, both off-road and on-road autonomous vehicles rely heavily on software and connectivity to operate safely. Unfortunately, as with any connected device, autonomous vehicles can be vulnerable to cyberattacks. As the technology continues to evolve, protecting a vehicle's software and communication systems from cyber threats is critical to ensuring the safety and integrity of autonomous transportation, whether on a paved road, a dense forest, or a construction site.

A threat actor that compromises a vehicle's software or communications system and achieves unauthorized access to a vehicle can potentially result in data theft, remote command and control operations, collision, injury, or even loss of life. This is especially true of military applications, where ensuring the cybersecurity of autonomous off-road vehicles is paramount to protect not only the safety of passengers, but also the integrity of the mission.

As it stands, however, cybersecurity for autonomous vehicles is still immature when compared to the protection capabilities of an enterprise environment. The complexity of autonomous systems, combined with a lack of universal standards, makes ensuring the security of these vehicles a challenging task. As such, the potential for adversarial threats requires advanced security measures and constant vigilance.

A Zero Trust Approach

At Neya, we are taking a Zero Trust approach with autonomous vehicles to secure network communications, monitor endpoints, implement identity and access management, and implement cryptographic key management, to name a few examples.

Zero Trust is built upon the philosophy of "trust nothing, verify everything." Historically, cybersecurity protections have followed Defense-In-Depth, or Layered Security approaches which are based upon physical security concepts of building a bastion. With these security models, you have a trusted internal network and untrusted external network divided by a multi-layered perimeter. Threats are typically identified when these protection layers are penetrated. Instead, Zero Trust assumes that threats may be present both inside and outside the network perimeter.

Another way to look at this is that traditional security implementation models are system-centric, whereas Zero Trust is data-centric. This is a key component of understanding the importance of Zero Trust, since it is concerned with knowing: 1) what data you have; 2) where it is moving within and outside of your network; and 3) who is accessing it.

The threat landscape is always evolving; therefore, the attack surface is much wider than it ever has been. There is a constant escalation between threat actors and those defending against them. As security breaches are detected and investigated, leading to improved defensive measures, offensive actors are forced to develop novel techniques to circumvent enhanced protections. Additionally, IT and OT environments have grown more complex in the last decade. Most environments are now hybrid on-premises with cloud-based components, or multi-cloud. Add in the growing diversity of physical devices such as mobile phones, tablets, wearables, and other IoT devices, which are leading traditional security models to age out of relevancy to effectively protect data and the end-user. A point of vulnerability only recently considered is with autonomous systems, or in this case, autonomous vehicle systems.

With the growing complexity of environments and diversity of devices accessing networks in mind, Zero Trust aims to defend against these many modern use cases. Above all, you need to protect sensitive data. Zero Trust provides the framework to secure access to resources, regardless of the user or device's location with consistent and enforceable security policies. Implementing least-privilege access policies and encryption mechanisms, followed by continuous verification of both user and device identities, allows organizations to prevent unauthorized access to critical data assets. The goal is to reduce the attack surface available to threat actors. One critical piece of Zero Trust is focused on continuous monitoring and behavioral analysis to detect anomalies and suspicious activities in real-time.

Real-Time Threat Identification

To be effective, cyber autonomy must be able to intelligently identify risks and take action to mitigate potential threats to autonomous vehicle missions. It must be completely self-contained, capable of autonomously detecting, reporting, and defending against threats that can exploit or disrupt a mission. By implementing a suite of behavioral analytics to baseline an expected, normal state-of-vehicle operation, we can leverage anomaly-detection techniques that will function as the "intelligent" subsystem, which then inform the decision-making capability of a cyber autonomous system.

The lifecycle of an autonomous vehicle is in three stages: Pre-Mission, Mission Operation, and Post-Mission. As one might expect, pre-mission routines are focused on defining the assets and mission objective. The vehicle will need to pass a pre-mission checklist for it to be authorized for operation. From a cybersecurity perspective, we need to ensure that each boot-up process is from an expected state to mitigate the potential for unauthorized software or malware usage.

Another example is to ensure that all OS and software is patched and up to date before the mission begins. Post-mission routines are focused primarily on reporting notable events and maintenance. All cybersecurity anomalies, events, and responses will be reported via an analytics dashboard within Neya's Mission Planning and Management System (MPMS). Additionally, bulk forensic data is captured and made available for authorized personnel. Securely updating the OS and software is also a crucial step in the post-mission routine, as the time to perform this task may cause significant delays when performed during the pre-mission routine.

Mission operation is the most complex stage of the autonomous vehicle lifecycle. Consider how an autonomous vehicle operates using perception and sensing to determine a path of least resistance. The perception and planning systems work to identify anomalous objects that serve as obstacles that cause the vehicle to change direction or operation for optimal traversal. Conceptually, cyber anomaly detection is remarkably similar. Sensors are placed within the vehicle network and its endpoints to detect digital signals of anomalous activity, instead of detecting a physical anomaly using RADAR or LiDAR as sensors.

Relevant data is an absolute necessity for anomaly detection to be successful. It needs to be structured, categorized, and labeled for effective aggregation and consistency to ensure data integrity for the subsystem responsible for processing it. An analytic baseline to determine what is normal or expected is required once the data is understood and organized. A simple example is measuring the network flow volume (i.e., could be bytes, packets, transactions) between two nodes within a vehicle. An anomaly will be reported if the network flow volume increases or decreases an order of magnitude away from what is recorded as normal in the established baseline for that analytic. After extensive testing to determine specific analytics to measure and to improve baseline accuracy, it is ready to begin field operations. The confidence threshold for positively identifying a cyber threat should also improve as more data and telemetry is collected and processed with each mission.

Furthermore, just as the vehicle autonomy system determines a response to physical anomalies, the autonomous system also will need to respond accordingly to a perceived cyber threat. For example, a threat actor attempts to establish unauthorized command and control of an autonomous vehicle using a rogue Operator Control Unit (OCU). There are several methods of protection, including defensive hardening to mitigate this attack vector, but in the case of a breach of defense, a standard operating procedure needs to exist to respond to this detected threat. In enterprise environments, this is handled by a person or group of people. An autonomous vehicle, on the other hand, is not expected to have trained personnel to respond.

Evaluate and Enforce

At Neya, we are introducing the Cyber Autonomous Response and Recovery System (CARRS) to autonomous vehicle platforms to solve this problem. CARRS is a kit that will be attached to the vehicle's autonomy stack. Its role is to evaluate and enforce Zero Trust policies and actively respond to detected high fidelity threats. CARRS will dynamically issue vehicle profile or configuration changes during a mission in the case of a security policy violation or detected threat. It may determine that turning off the radios is an appropriate response or push a change in network policy to deny traffic from a rogue OCU device, as previously noted in the above example.

The capabilities of autonomous vehicles are ever evolving, and, at the same time, so is the threat landscape. Adversaries are ever vigilant and novel in their approach to cyber-attacks. The complexity of autonomous vehicles, both on-road and off-road, underscores the need for continued vigilance in addressing potential vulnerabilities.

About the Author

Joseph Hladik is the Cyber Group Lead at Neya Systems and has been with Neya since 2023. During this time, Hladik has led various projects, including cyber autonomy, a solution-based software program that will be added to mission planning to mitigate cyber threats during deployment. Prior to Neya, Hladik worked as the Director of Threat Research and Intelligence at Counterflow AI, where he furthered the knowledge and detection of threat actor Tactics, Techniques, and Procedures (TTP) leveraging Machine Learning Algorithms (MLA) and Behavioral Analytics. Before his role at Counterflow AI, Hladik worked at Mandiant as the Regional Manager for the U.S. Northeast and Canada regions.

Hladik can be reached through the Neya company website www.neyarobotics.com

Navigating the Perilous Waters of Supply Chain Cybersecurity

By Kenneth Moras

Introduction:

In today's interconnected business environment, reliance on innovative vendors and open source solutions is inevitable. However, these supply chains also stand on the frontline in the battle against cyber threats. As I delve into the Verizon 2024 Data Breach Investigations Report (DBIR), it re-emphasizes the theme that underscores a critical vulnerability many businesses overlook: the supply chain. This blog explores the vulnerabilities within supply chains highlighted in the report and outlines steps companies can take to enhance their defenses.

The Growing Threat to Supply Chains:

Supply chain attacks are particularly dangerous because they exploit trusted relationships between businesses and their suppliers. The DBIR notes a significant uptick in incidents where breaches were facilitated through third-party software vulnerabilities. These vulnerabilities not only expose individual companies but can ripple through the entire supply chain, causing widespread damage. The report

reveals a concerning trend where supply chain interactions, primarily through third-party software, have become significant breach points. The infamous instances of software like SolarWinds and the less-discussed but equally threatening 3CX, where malicious updates led to widespread security breaches, serve as stark reminders of this vulnerability.

Vulnerabilities in Third-Party Integrations:

As businesses integrate more third-party solutions into their operations, the attack surface widens. The report shows how attackers are increasingly targeting less-secure elements within the supply chain to deploy ransomware or conduct extortion operations. High-profile breaches involving software like SolarWinds and 3CX exemplify how quickly and extensively damage can spread through these vulnerabilities.

Vulnerabilities Introduced in Open Source Dependencies:

The recent CVE-2024-3094 vulnerability in XZ Utils involved a backdoor that enabled unauthorized remote code execution (RCE) and could bypass SSH authentication. This critical flaw was surreptitiously introduced by a trusted maintainer over a two-year period. If not identified and mitigated in a timely manner, this vulnerability could have allowed attackers to gain full control of affected systems, potentially leading to widespread unauthorized access, data breaches, and disruption in services across numerous Linux distributions where XZ Utils is deployed.

The Role of Third-Party Software:

The DBIR indicates that 15% of breaches involved third-party software vulnerabilities, a notable increase from previous years. This trend shows a growing reliance on external vendors and the inherent risks associated with it. Ransomware and extortion attacks often exploit these vulnerabilities, compromising not just a single entity but entire networks connected through supply chains.

Strategies Used by Industry to Combat Risks Introduced by Open Source:

A Software Bill of Materials (SBOM) is increasingly requested by organizations seeking to evaluate third-party solutions before procurement. This growing trend reflects a heightened awareness of cybersecurity risks associated with software supply chains. An SBOM provides a detailed inventory of all components, libraries, and modules contained in a software product, along with their versions and dependencies. This transparency enables organizations to identify potential security vulnerabilities, compliance issues, and operational risks inherent in third-party software.

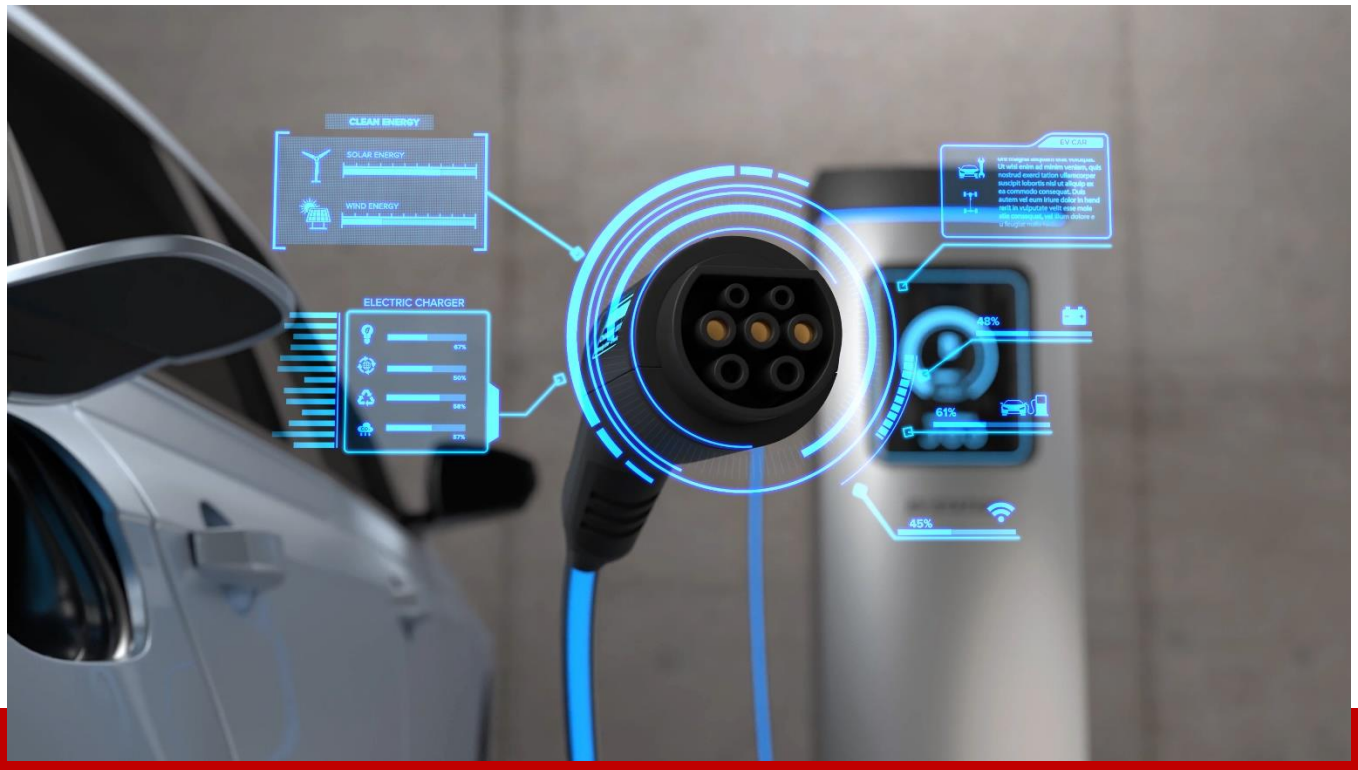
Conclusion:

As supply chains become increasingly digitized, their security implications cannot be overstated. The insights from the DBIR 2024 serve as a reminder that in the digital age, our defenses are only as strong as the weakest link in our supply chain. Proactive measures, continuous monitoring, and collaborative security efforts are essential to safeguard our interconnected business ecosystems.

About the Author

Kenneth Moras is a cybersecurity governance risk and Compliance leader with 15+ years of experience. He has implemented and scaled GRC programs at notable organizations such as Meta, Adobe and Plaid. His expertise also extends to cybersecurity consulting for Fortune 500 companies during his tenure at KPMG. He holds various certifications, including CISSP, CISA, ISO 27001 LA, CDPSE, CEH, CHFI, and CCNA. Kenneth enjoys staying up-to-date with offensive strategies used by attackers and building proactive risk management programs that serve as business enablers

Kenneth Moras can be reached online at LinkedIn (https://www.linkedin.com/in/kennethmoras/)



How Improving EV Charging Infrastructure Can Bolster US Cybersecurity Measures

By Elaina Farnsworth, Co-founder & CEO — SkillFusion

The surging popularity of electric vehicles (EVs) is marking a strong push toward overall sustainability for the United States. However, as EV adoption becomes more widespread, the need for a reliable and secure EV charging infrastructure becomes more apparent.

EV charging stations are increasing their capabilities year by year, such as expanded power delivery systems and better networking and sharing of data analytics. As innovations surrounding the electrification of transportation continue to emerge, concern over the political, economic, and logistical risks associated with cyberattacks grows.

Cybercriminals are becoming savvier, and attacks that target EV charging stations can affect crucial services from the supply chain to medical services. Securing the EV charging infrastructure and assuring that the new EV-aligned workforce has training in cybersecurity specifics will be necessary considerations to keep the EV revolution going and strengthen the country's trust in the EV charging network.

A secure network

As part of its Infrastructure Bill, the Biden Administration pledged to build 500,000 new EV charging stations by 2030. To bring this plan to fruition, the expanded EV-adjacent workforce promised by government officials will need to focus on skill-building in EV charging station cybersecurity.

We know that cyberattacks on the current and future EV charging infrastructure are bound to occur. Cybercriminals are improving their methods day by day, and cybersecurity professionals must do the same. What is critical is an understanding of how a robust EV infrastructure supports overall national security.

To safeguard against the onslaught of cyber threats that are bound to come against a network as widespread as the proposed EV charging network of the near future, specially trained technicians must employ the latest encryption protocols, authentication approaches, and secure communication channels. These cybersecurity best practices work to safeguard the charging infrastructure from unauthorized access that could bring the entire network down.

In addition, initiatives that seek to strengthen the EV charging infrastructure must include the integration of cybersecurity standards industry-wide. The creation and implementation of standards across the entire expanded network will ensure compliance and reliability, no matter the manufacturer or network.

Going forward, the expanded EV charging infrastructure will require advanced monitoring and detection of vulnerabilities that could lead to issues across the network. Measures such as AI-aided monitoring or digital twin technology could allow cybersecurity professionals to anticipate issues before they become catastrophic.

Lastly, any government initiatives that seek to expand the security of the EV charging network must include allowances for research and development. One constant of the sustainability movement is chance, and innovations are emerging at breakneck speed. Cybersecurity technologies such as firmware updates and ongoing solutions such as better intrusion detection systems will need to keep pace with the EV charging market.

On the road to secure energy independence

In the race toward zero emissions and more energy independence, all signs point to the US being on the right track. Cybersecurity for the EV charging infrastructure, both current and future, will play a critical role as we work toward more sustainable transportation.

A secure charging network will build trust in EV drivers. The current EV infrastructure has run up against some reliability challenges, with studies showing that 20% is inoperable at any given time. With better attention paid to training and deploying skilled technicians to support the current and planned charging network, reliability will improve over time. If the network's security can be included in those improvements, EV drivers will begin to have more faith in the network as a whole.

Strong cybersecurity measures will prevent disruptions in the network, assuring that people will be able to charge their vehicles. In addition, large fleets of electric vehicles being used to transport goods will be able to operate uninterrupted, supporting the national and global supply chain's goal of zero emissions.

EV charging networks are increasingly interconnected with energy grids. A more robust cybersecurity plan for the EV charging infrastructure means a more protected grid system, supporting a renewable energy system and promoting a sustainable energy ecosystem.

The road to energy independence and a more sustainable future will be paved by the cybersecurity professionals who serve as the strongest frontline defense against bad actors who are consistently improving their tactics. By remaining one step ahead of cybercriminals in innovation and security measure best practices, we can secure the EV charging network and allow the EV revolution to continue moving forward.

About the Author

Elaina Farnsworth is the Co-founder and Chief Executive Officer of SkillFusion, a cutting-edge customer success platform for electric vehicle service equipment (EVSE) operations and maintenance (O&M) providers. With a passion and career-long dedication to talent and workforce development and community engagement, Farnsworth is focused on growing a certified talent pool with SkillFusion to operate and maintain electric vehicle chargers and facilitate the growth of the charging network across the country. Prior to SkillFusion, Farnsworth was the CEO of The Next Education where she developed best-in-class continuing education and certification programs designed to upskill and reskill the workforce in automotive careers related to electrification, autonomy, and cybersecurity. She has created and led credentialing and certification programs for the defense sector, federal agencies, Society of Automotive Engineers (SAE), and other industry-leading private entities. Additionally, as a software developer, Farnsworth has a proven track record in bringing to market resource allocation platforms capable of just-in-time dispatching of resources.

Elaina can be reached online at https://www.linkedin.com/in/elainafarnsworth/and at our company website http://www.skillfusion.com/

Cybersecurity as a Service Market: A Domain of Innumerable Opportunities

Cybersecurity as a Service Market

By Aashi Mishra, Content Writer, Research Nester

The increased internet usage, all across the globe, is giving rise to cybercrime cases. Cybercrime is any unlawful activity that involves a network, computer, or networked device. The aim of attempting a cybercrime is to breach security and steal sensitive or valuable information. The attacks come in numerous forms such as phishing, hacking, identity theft, and software. Some of the statistics related to the cyber attacks are given as follows:

- By the year 2025, the cost of cybercrime will reach almost 10.4 trillion.
- In 2023, the maximum cost of a data breach occurred worth almost USD 5.10 million in the United States.
- In the year 2023, there was an 8.1% rise in weekly cyberattacks.
- Small businesses account for almost 43.1% of cyber attacks annually.

- Almost 33.5% of small businesses in the United States are at risk of cyberattack

This information is alarming and tech geeks are coming up with numerous solutions. One of the popular solutions is CSaaS, that is, CyberSecurity as a Service. In this blog, we will understand various aspects associated with the CyberSecurity as a Service market and its future growth aspects.

It has been estimated that the addressable market in cybersecurity might reach almost USD 1.5 trillion to almost USD 2.1 trillion. The priorities of shielding businesses have become of prime importance for the market players. Let us understand how cyber security is becoming an important aspect for various businesses.

1- Cyber security in healthcare

Recently, news surfaced on the internet that a Southern California-based medical group became the victim of a cyber attack in 2022. The average cost of a healthcare breach in the United States is almost USD 10.9 million. Healthcare organizations are susceptible to various cyber attacks for reasons such as,

- The advent of digitalization in healthcare is causing more attacks
- Rise in the healthcare ecosystem based on the interconnected medical devices
- Growth in security talent shortage
- Presence of a large user base

In today's digital age, numerous healthcare organizations are incorporating Cyber Security as a Service Market which helps in eradicating cyber attacks.

2- Cyber Security in IT and Telecom

The telecommunication industry is considered to be a crucial infrastructure that needs to be fabricated to withstand numerous types of cyber attacks. For numerous years, telecommunication companies have been a prime target for cybercriminals. Cyber security in telecom helps protect from data breaches and malicious attacks.

3- Cyber Security in Defence

In February 2024, news of 2 Iranian military ships being attacked by United States cyberattackers surfaced on the internet. It shows the rising importance of cybersecurity in the domain. Various governments are embracing cybersecurity to protect important data from malicious attacks.

Similarly, domains such as retail, BFSI, defense, automotive, education, etc., are adopting cybersecurity as their priority safety measures.

Although traditional cybersecurity differs from cybersecurity as a service. As per the budget, size, and regulatory compliance requirements, several approaches are required. Organizations are finding it tedious to rely completely on themselves. The conventional method of fabricating an internal security

team is to hire an experienced security staff who are dedicated to performing cyber security duties. While CSaaS is an option where the company outsources the security facility. A survey found that almost 72.1% of businesses find CSaaS solutions critical for their customer strategy. Let us now understand cyber security as a service market growth aspect.

CSaaS Market Analysis:

The Cyber Security as a Service Market size is projected to cross almost USD 140 Billion by the end of the year 2033, growing at a CAGR of 13% during the forecast period. Also, in 2022, the CSaaS market garnered almost USD 72 billion. Some of the growth-propelling factors for the CSaaS market are:

- The surge in incidences of data breaches and cyberattacks
- The rise in cybercrime on social media platforms
- Technological advancements in cyber security services
- Surge in fraudulent money request attacks
- Rise in the number of Internet users

Some of the challenges in the market growth are lack of training and inadequate workforce, limited security budget among SMEs, and lack of interoperability with the information.

The market in North America currently accounts for the maximum share of the revenue of the worldwide market. The growth of the market can be attributed to the high level of digitalization and the surge in the number of connected devices in the countries is projected to remain growth-propelling factors. Other than this, Asia-Pacific markets are also expected to continue to thrive due to the increasing number of government initiatives. Also, the rising number of reliable and cost-effective measures is acting as a catalyst in the growth of the market. Some of the leading companies in the domain of CSaaS market are Cisco Systems, Inc., IBM Corporation, Microsoft, Check Point Software Technologies Ltd, Oracle, Trend Micro Incorporated, Cyber-Ark Software Ltd, FireEye, Imperva, and ProofPoint Inc.

In a nutshell

The cyber security as a service market holds lucrative opportunities for growth in the future. However, for the budding as well as new market players, it is crucial to understand various market intricacies. These factors are imperative for market players to make prudent business decisions. An exhaustive market research report consists of various parameters such as future growth aspects, market constraints, growth driving factors, regional analysis etc. These factors also help the market players to carve make themselves a niche.

Source: https://www.researchnester.com/reports/cyber-security-as-a-service-market/4538

About the Author

Aashi Mishra an experienced research writer, strategist, and marketer with a demonstrated history of research in a myriad of industries. I love to distill complex industrial terminologies of market space into simpler terms.

Aashi Mishra can be reached at https://www.researchnester.com/


EVENTS

5TH CYBER SECURITY FOR ENERGY AND UTILITIES CONFERENCE

FOSTERING CYBER RESILIENCE:
SAFEGUARDING ENERGY AND UTILITY OPERATIONS

DATES: 5 – 6 JUNE 2024 | **WORKSHOP:** 4 JUNE 2024

ABU DHABI, UAE

HOSTED BY

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

SCAN TO BLOCK YOUR SPACE

SUPPORTING PARTNERS

ORGANIZED BY

cybersecurityinenergyandutilities.com

e-CyberHealth 2024

Diagnostics – Hospitals – Pharmaceuticals

Athens - 3 July 2024 - Greece

The Digital transformation in the Healthcare industry is in a continuous process of evolution.

The key actors, Healthcare Organizations, Pharmaceutical Companies, Healthcare Professionals as well as Patients, are on the alert for the security of medical data and electronic processes.

The aim of the #eCyberHealth24 Conference is to raise awareness and strengthen the collaboration of all stakeholders in the e-Health environment, in addressing current and future CyberSecurity challenges.

Stay tuned at **www.e-cyberhealth.eu**

Media Partner

CYBER DEFENSE MAGAZINE

Organizer

ZOMIDEA design & services ltd
T: +357 22 515561
E: zomidea@cytanet.com.cy
W: www.zomidea.eu


black hat®
USA 2024
AUGUST 3-8, 2024
MANDALAY BAY/LAS VEGAS
informa tech

Register for your FREE pass

www.emergencytechshow.com


DUBAI
ITS World Congress
16 -20 September 2024
Mobility Driven by ITS
Up to 20.000
ITS Experts
+500
Innovations Showcased
+800
International Speakers
+200
Expert Sessions
REGISTER NOW
Join us in shaping the future of ITS and Smart Mobility at the ITS World Congress in Dubai! For more info, itsworldcongress.com.
16-20 September 2024
Dubai World Trade Centre
ORGANISED BY
ERTICO
ITS EUROPE
CO-ORGANISED BY
ITS AMERICA
ITS
HOSTED BY
RTA
SUPPORTED BY
DUBAI
DXB
BestCities
GLOBAL ALLIANCE

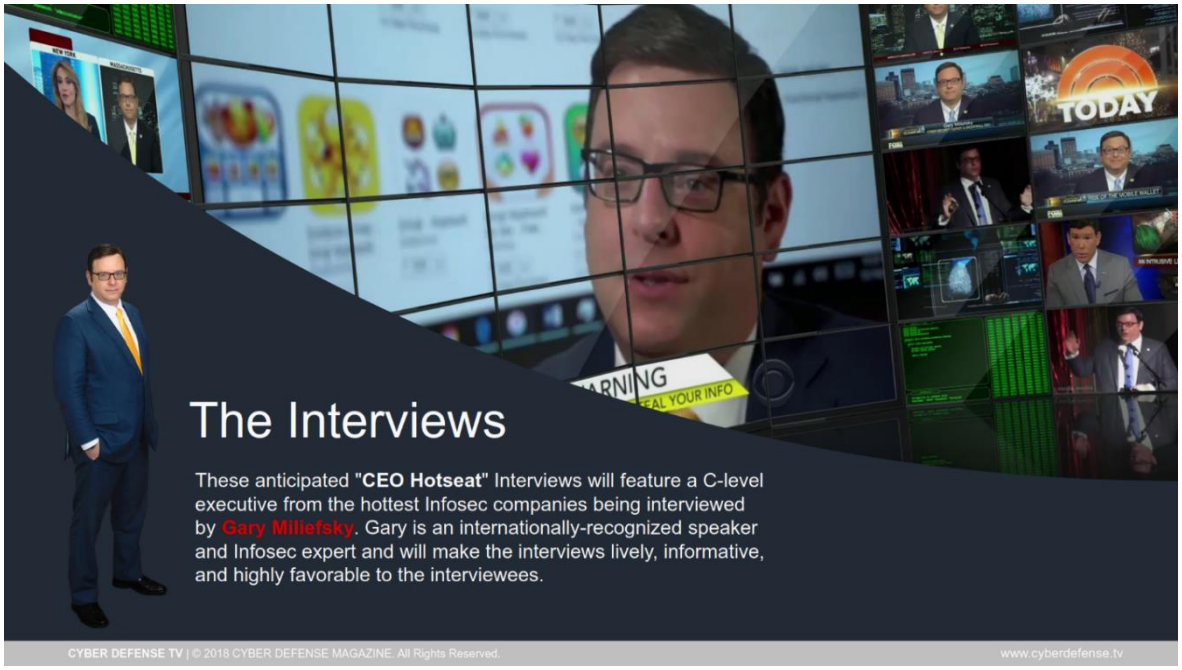
CYBER DEFENSE TV

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.

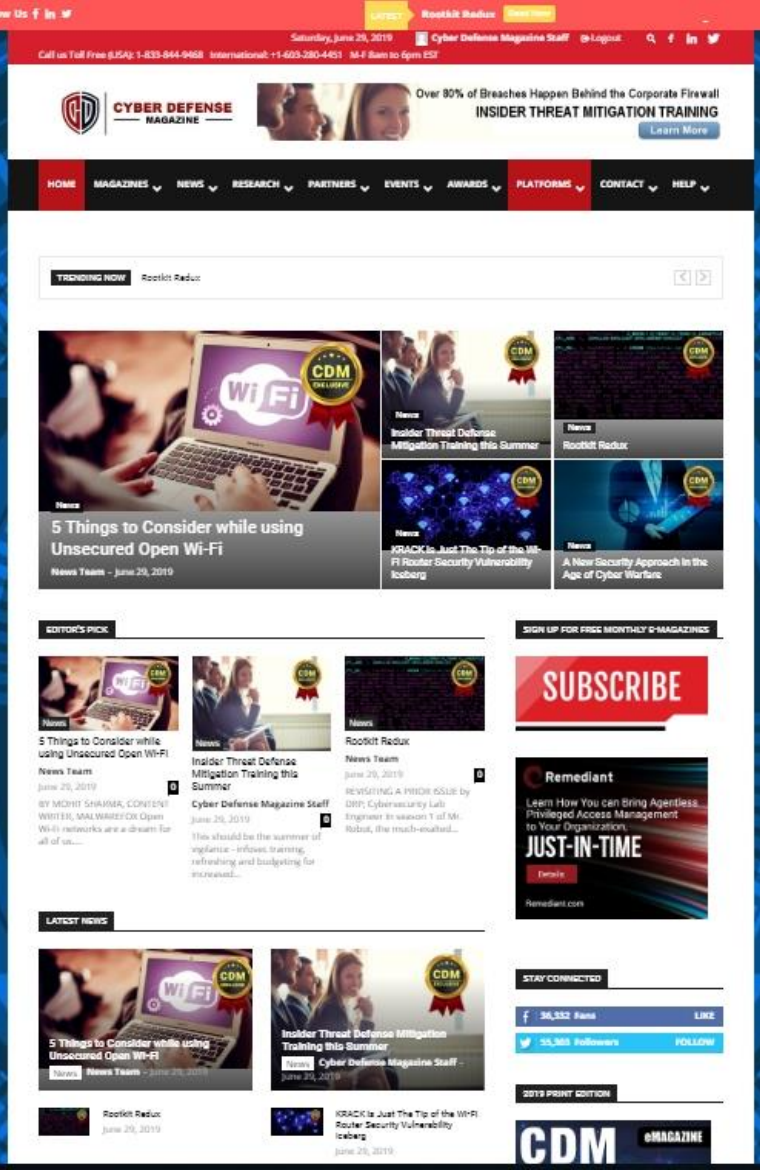
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 06/03/2024



Books by our Publisher: [Amazon.com: CRYPTOCONOMY®, 2nd Edition: Bitcoins, Blockchains & Bad Guys eBook : Miliefsky, Gary: Kindle Store (with others coming soon...)]

12 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. We successfully launched https://cyberdefenseconferences.com/ and our new platform https://cyberdefensewire.com/

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensewire.com
www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

*** with help from writers and friends all over the Globe.**