CYBER DEFENSE MAGAZINE

eMAGAZINE

APRIL 2021

In This Edition

MORE INSIDE!

Contents

Contents

@MILIEFSKY

From the Publisher…

New CyberDefenseMagazine.com website, plus updates at CyberDefenseTV.com & CyberDefenseRadio.com

Dear Friends,

The trends we observed and noted in last month's magazine have, not surprisingly, continued and expanded. The new challenges we face continue to grow in magnitude and reach. Fortunately, we are able to bring to bear not only our own internal resources, but also valuable commentary from our many contributors.

We are seeing new and sometimes challenging government responses to continuing COVID-related threats. These will no doubt have consequences, both intended and unintended, in workplace practices and security measures.

An example since last month is the expected additional restriction on air travel, which apparently will extend to domestic air travel and even other public transportation. These more stringent measures to confront the pandemic on the travel front will apparently require proof of vaccination or quarantine.

We can, of course, expect this to result in more pressure on remote workers, with a disproportionate effect on those who receive and manage sensitive data. Both employers and workers will experience constant need to update and test the efficacy of cyber security measures in order to avoid costly breaches.

At Cyber Defense Media Group, we are fortunate to count on perceptive and helpful articles from our many knowledgeable contributors. Our readers have shown by the growth in their ranks that they too rely on this valuable actionable information.

We are pleased to recognize Cyber Defense Magazine and the related resources of Cyber Defense Media Group, as essential tools for cybersecurity success.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS

CEO, Cyber Defense Media Group

Publisher, Cyber Defense Magazine

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

InfoSec Knowledge is Power. We will always strive to provide the latest, most up to date FREE InfoSec information.

From the International Editor-in-Chief…

As a close observer of international trends in cybersecurity, among my primary points of focus are the relative compatibility (or incompatibility) of laws and regulations in different jurisdictions, and recognition of the practical fact that compliance with these laws and regulations do not necessarily relieve liability in the event of a data breach or malware/ransomware exploit.

In this same vein, we are seeing the transition from working in an office environment to working from home (WFH) as a long-term, rather than temporary, migration.

Internationally, there are effects on digital workers which may not have been foreseen, but are becoming apparent in areas such as stress and health (physical as well as mental). The 24/7 nature of international operations appears to create more anxiety as people realize that sending an asynchronous email to someone in a distant time zone may no longer be an acceptable response to an operational inquiry – expectations for immediate substantive responses are becoming the norm.

Under these circumstances, we do well to be aware of these personal and organizational stresses, and make allowance for them as we lead our daily digital lives.

As always, we encourage cooperation and compatibility among nations and international organizations on cybersecurity and privacy matters.

To our faithful readers, we thank you,
Pierluigi Paganini
International Editor-in-Chief

@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.

PRESIDENT & CO-FOUNDER
Stevin Miliefsky
stevinv@cyberdefensemagazine.com

INTERNATIONAL EDITOR-IN-CHIEF & CO-FOUNDER
Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

US EDITOR-IN-CHIEF
Yan Ross, JD
Yan.Ross@cyberdefensemediagroup.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

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

PUBLISHER
Gary S. Miliefsky, CISSP®

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

9 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:

CDMG B2C MAGAZINE
B2B/B2G MAGAZINE TV RADIO AWARDS
PROFESSIONALS WEBINARS

Welcome to CDM's April 2021 Issue

From the U.S. Editor-in-Chief

We recently passed the 1-year mark since the formal announcement of the COVID-19 pandemic by the World Health Organization (WHO). It is apparent from the subjects and perspectives of the authors submitting articles for Cyber Defense Magazine that the digital effects of this health emergency are going to be with us for well into the foreseeable future.

While there are no fully-vetted statistics on the migration from the office environment to work-from-home (WFH) scenarios, anecdotal evidence indicates that the vast majority (perhaps as much as 80%) of workers who now work from home would prefer to avoid ever returning to the traditional office.

A brief scan of the topics of this month's Cyber Defense Magazine shows that the thrust of the articles does indeed relate to the consequences or projections of cybersecurity threats arising out of changes based on social distancing, lockdowns, and other responses to the spread of the virus.

In our capacity as the publication with focus on emerging trends and solutions in the word of cybersecurity, we commend your attention to the valuable guidance provided by our expert contributors.

Wishing you all success in your cyber security endeavors,

Yan Ross
U.S. Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & US Editor-in-Chief for 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 via his e-mail address at yan.ross@cyberdefensemediagroup.com


SPONSORS

THETA432™

Prepare Against Cyber Attacks!

With Dynamically Defined Defense™ (3D).

See If I Need Cyber Defense

Cyber Defense

Best-in-Class Cyber Defense Services, operated 24 / 7 by Industry-Leading Professionals from around the world.

IRAAS + TRU-A™

Incident Response as a Service provided by our dedicated world class Threat Operation Center.

Digital Forensics

You need answers into what happened and how to fix it. You want to know who accessed what, when and how.

Remote Monitoring

Our Threat Operation Center Provides Remote Monitoring and Response Services with dedicated Analysts at your side.

As seen in

THE WALL STREET JOURNAL.

abc NEWS

CIO Review

I.R.I.S.™ INCIDENT RESPONSE INVESTIGATION SYSTEMS

TRU-A THREAT RESEARCH UNIT ALPHA

AI acquisition international the voice of modern business - est. 2010

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020

THETA432™ BEYOND VISIBILITY™

Next Gen
Managed Prevention, Detection And Response Services (MPDRS)

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020

THETA432™ BEYOND VISIBILITY™

Cutting Edge
Cyber Defense Services

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020

THETA432™ BEYOND VISIBILITY™

Hot Company
Cyber Security Services

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020

THETA432™ BEYOND VISIBILITY™

Publisher's Choice
Cyber Threat Services


FOCUS ON YOUR BUSINESS, NOT YOUR EMPLOYEES' CYBER HABITS.
CYBERSECURITY DONE RIGHT.
FluencySecurity.com
Fluency

Do you check the boxes with your cybersecurity?

- [x] **Leadership Prioritizes Cybersecurity**
- [ ] Assessments
- [ ] Plans
- [ ] Policies
- [ ] Procedures
- [ ] Training
- [ ] Education
- [ ] Testing
- [ ] Scanning
- [ ] Monitoring
- [ ] Response

Antivirus

Protects devices against known infections

Firewalls

Protects networks against unauthorized access

DEFENDIFY

Cybersecurity. *Simplified.*

Protects organizations against diverse threat landscape

What's Your Cybersecurity Strength?

A+ A A- B+ B B- **C+** C C- D+ D D- F

Find out in 3 minutes

www.defendify.io/mygrade

WORK ON THE FRONT LINES PROTECTING AMERICAN INTERESTS

Air Force Civilian Service (AFCS) has hundreds of civilian cyber security and IT professionals working to safeguard Air Force facilities, vital intelligence, and digital assets. We're looking for the best and brightest to help us stay ahead of this ongoing threat.

In fact, AFCS is currently hiring cyber security specialists, information technology specialists, information security specialists, software developers, software engineers, computer scientists, and computer engineers. These are challenging and rewarding positions that put you at the heart of our mission in cyberspace. Our systems are some of the most complex in the world, and we need the best in the business to keep our infrastructure and digital information secure.

Consider AFCS. You'll nd a supportive and inclusive workplace, where excellence is rewarded, and work-life balance is a priority. Factor in great benefits and you'll see why AFCS is a place where you can excel. At 170,000 strong, we are a force to be reckoned with. Find your place with us and watch your career soar.

AFCivilianCareers.com/CYBER | #ItsACivilianThing

Equal Opportunity Employer. U.S. Citizenship required. Must be of legal working age.

AIR FORCE CIVILIAN SERVICE

Forces. Joined.

cythereal

Lucio Frega, Threat Researcher
Deutsche Telekom - Cyber Threat Intelligence

DTAG-CTI (Deutsche Telekom - Cyber Threat Intelligence) protects clients against cyber-attacks worldwide.

Like us, the adversaries too have cyber-experts. They continuously enhance their malware attacks with stealth and anti-forensics capabilities. This increases our overall risk and also the cost of detection and remediation.

For example, repacked malware strains evade endpoint's protection, fluxed C2s bypass SIEM, and obfuscations fool reversing.

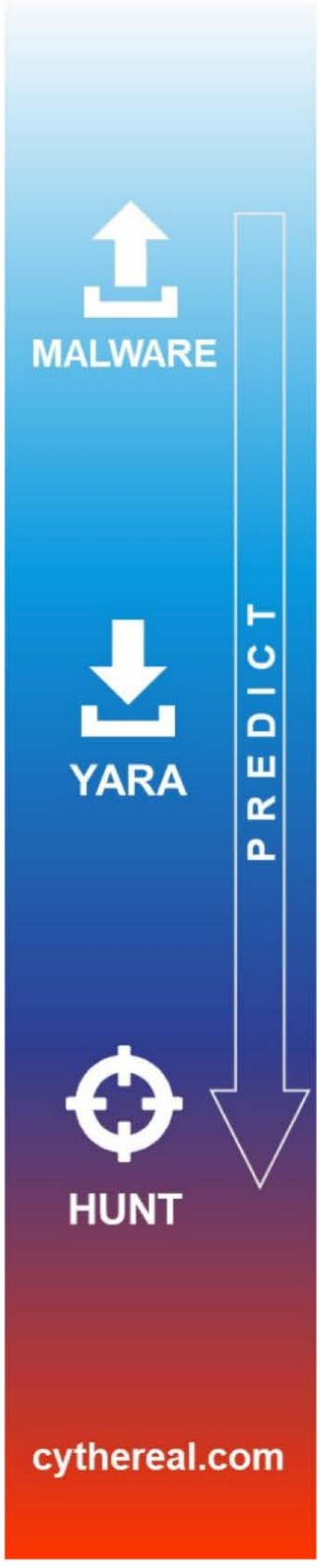
We can cope with this in spite of the high cost. However, it all amounts to nothing if, by the time a defense is erected, the attack has reshaped and shifted direction again, turning those defenses obsolete.

We in DTAG-CTI have erected predictive defenses using malware's code-similarity.

This predictive layer goes beyond network activity, behavior, metadata and state-of-the-art technologies. We match binaries using Cythereal's automatically generated YARA rules, unearthing previously unseen strains despite reshuffling, repacking, and other evasions. These predictive defenses nail the malware "in the bud," before it has had a chance to spread or even to report to its C2.

As an extra value, these early detections also empower early identification. We learn from the start who is against us and hunt for associations regardless of their obfuscated binaries, dissimilar metadata, IOCs, and payloads.

Together with the professionalism and commitment of our teams and partners, we have found in the expertise, dedication, and engagement of Cythereal a very powerful and astounding ally that brings threat hunting and cyber-defense to a superior level.



About the Author/Disclosure

Lucio Frega is a computer forensic examiner certified by IACIS (International Association of Computer Investigative Specialists). He has over 40 years of worldwide experience in IT/OT security in Banks, Pharma, Telcos and the energy sector. Lucio is not affiliated with Cythereal. His comments are not to be construed as the official posture of any stakeholder but himself.

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

***"At** Stony Lonesome Group, we believe that Freedom Is Not Free and we do not take it for granted. SLG is a pioneer and thought leader in Mission Focused Investing protecting American Exceptionalism and National Security by investing in a vital areas of Cybersecurity, Big Data Analytics, and Artificial Intelligence. "*

Sean Drake
Managing Partner
Stony Lonesome Group LLC
203-247-2479
www.stonylonesomegroupllc.com

By the time an attacker tastes the difference, their presence is known.

"Attacker mistakes are made when they cannot distinguish real from fake."
Tony Cole, CTO Attivo Networks

DECEPTION-BASED THREAT DETECTION

Detecting threats needs to be comprehensive, however it doesn't have to be complicated. Designed for simplicity, Attivo Networks brings uncertainty to the mind of the attacker, redirecting them away from the target assets and providing defenders with high-fidelity alerting that is backed with actionable attack and forensic data on malicious activity and insider policy violations.

Attivo NETWORKS

Deceive. Detect. Defend.

Learn more at attivonetworks.com/ebook

Setting the Standard

in Cyber Defense Training & Education

Transform your cyber defense capabilities with customized training. Regent's Institute for Cybersecurity will help you develop your workforce credentials, manage your cyber risks and defend your assets.

CORPORATE | GOVERNMENT | MILITARY | EDUCATION

- Powerful Hyper-Realistic Range Simulation
- Industry Certifications
- Executive & Senior Leadership Cyber Workshops
- Associate, Bachelor's & Master's Programs

Regent's B.S. in Cybersecurity has received NSA and DHS designation.

Learn More

regent.edu/cyber | 757.352.4590

REGENT UNIVERSITY | Institute for Cybersecurity

OneTrust

Privacy Management Software

World's #1 Most Widely Used Privacy Management Software

For Privacy, Security & Third-Party Compliance

Solutions to Comply with the CCPA, GDPR & Global Privacy Laws & Security Frameworks

Privacy Program Management:

- **Maturity & Planning:** Compliance Reporting Scorecard
- **Program Benchmarking:** Comparison Against Peers
- **DataGuidance Research:** Regulatory Tracking Portal
- **Assessment Automation:** PIAs, DPIAs & Info Security

Marketing & Privacy UX

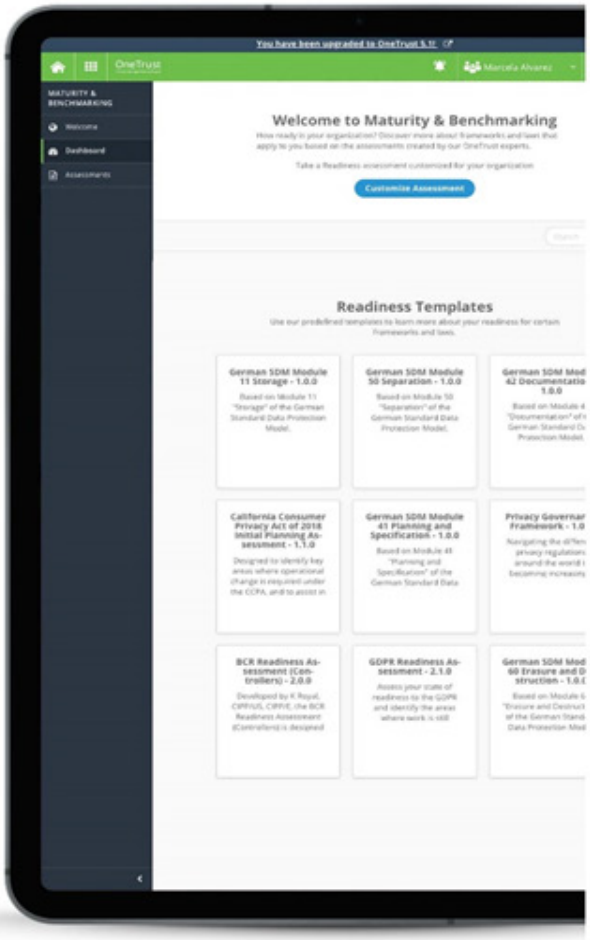
- **Cookie Compliance:** Website Scanning & Consent
- **Mobile App Compliance:** App Scanning & Consent
- **Universal Consent:** Consent Receipts & Analytics
- **Preference Management:** End User Preference Center
- **Consumer & Subject Requests:** Intake to Fulfillment
- **Policy & Notice:** Centrally Host, Track & Update

Third-Party Risk Management

- **Vendorpedia Management:** Assessment & Lifecycle
- **Vendorpedia Risk Exchange:** Security & Privacy Risks
- **Vendorpedia Contracts:** Contract Scanning & Analytics
- **Vendorpedia Monitoring:** Privacy & Security Threats
- **Vendor Chasing Services:** Managed Chasing Services

Incident & Breach Response

- **Incident & Breach Response:** Intake & Lifecycle Management
- **DatabreachPedia Guidance:** Built-in guidance from 300 laws



GET STARTED TODAY | ONETRUST.COM/FREE-EDITION

LEARN MORE ABOUT ONETRUST | REQUEST A DEMO | ONETRUST.COM

Now More Than Ever, You Need To Be Connecting With

Customers

Influencers

Media

At Vrge Strategies, we've been making connections that businesses build around for more than a decade.

Cybersecurity companies (from VC-funded startups to the Fortune 500) and global nonprofits count on us every day to deliver results that lead, influence, as well as spark conversations and new business.

Isn't it time you maximized the value of your **strategic communications?**

Come talk to us, we'd love to connect.

Email Adam Benson
adam@vrge.us
or visit us at
www.vrge.us/cybersecurity

vrge
Navigate the Politics of Disruption

Database Cyber Security Guard

Don't be the next data breach. Equifax paid $575 million, British Airways $230 million and Marriott $124 million in fines.

Prevents confidential data theft by Hackers, Rogue Insiders, Phishing Emails, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks.

Product Features

- Detects Informix, MariaDB, MySQL, Oracle, SQL Server and Sybase data theft within milliseconds and shuts down Hackers immediately.
- Advanced SQL Behavioral Analysis of the database query activity learns the normal query patterns and detects database data theft.
- View all suspicious database activity and attempted data theft.
- Supports key GDPR compliance requirements. Non-intrusive detection of data theft. Runs on a network tap or proxy server.

Get a FREE COPY now.

www.DontBeBreached.com/Free

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


ARTICLES

Cyber Defense 101 for 2021 and Beyond: The Case for Liberating Network Management

A smart, secure separate management plane can help organizations defend against increasingly severe cyber threats

By Todd Rychecky, VP of Americas at Opengear

Whether it's a phishing scam targeting unsuspecting employees, malware on critical infrastructure or another type of malicious breach, cyber-attacks have been an all-too-familiar danger, and numbers are only growing. Of course, with each passing year, these threats not only increase in quantity, but also complexity and sophistication.

For instance, the recent explosion of work from home network traffic and mainstream adoption of cloud services has led to many telling trends, such as a 630% increase in threats targeting cloud services. And similar trends are likely to continue as digital ecosystems continue to grow with a plethora of new and increasingly sophisticated connected devices.

So, what can be done to protect against these increasing threats? One relatively simple step could be to separate network management from the primary network processing user data traffic.

The costs of a vulnerable network management plane

When organizational networks are not resilient, businesses are often blindsided by attacks, leaving everyone scrambling and operations crashing to a halt. Adding gravity to the situation, costs from an outage could be crippling. In fact, an Opengear survey recently showed that nearly 1/3 of organizations lose more than $1 million from network outages each year.

The primary production network is where users are checking their email, where a connected device may be collecting data and generally where most network traffic is flowing. If management can be compromised on this network, the chances and severity of a breach multiply exponentially because it exposes management to attacks from anyone that can connect to a vulnerable device.

Without a separate management plane, crucial personnel and systems can get locked out or even taken over during disruptions and attacks, meaning longer, more impactful outages or a total meltdown. Even something as small as a fake download link leading to malware, for example, could open the door for malicious code, theft of data or long periods of downtime.

By using a separate network management connection to reach console ports, known as out-of-band (OOB) management, network engineers or admins can reach any core or edge location in a network, whether the production network is experiencing issues or not. This relatively easy-to-implement step can drastically improve visibility into the status of connected devices and enable real-time issue resolution to prevent and thwart cyber-attacks.

Establishing a separate line for network management

There are several options for implementing a separate connection for network management. For instance, some may use a cable modem, while others may use a second Ethernet interface built on an entirely separate network. However, the most flexible and scalable option is to use a 4G LTE cellular connection, which can be made highly secure with several precautionary measures, like IPsec VPN tunnels and other protocols. While it could take weeks to install something like an MPLS circuit for an independent management plane, a cellular connection can be activated in hours from a remote location. This enables organizations with multiple facilities to quickly set up separate connections and even equip them with smart capabilities like proactive monitoring and alerts, automatic failover and near-instant remediation.

Due to the ease of being able to set up a separate network management plane over cellular, it is becoming a more valuable and widely accessible tool to defend against the growing threat landscape. Adding to this, tools like TPM chips that prevent hardware tampering and zero touch provisioning capabilities are enabling a wave of secure remote deployments that enable anyone to quickly set up a new site.

The power of a “smart” management plane

Establishing a separate network management plane to safeguard core data center operations has always been important for network management and security. But as trends like IoT, SD-WAN, remote work and edge computing ramp up, a separate connection with smart capabilities is becoming ever more critical.

Organizations are now managing more geographically dispersed network nodes, which each present new vectors for actors to breach, as well as new vulnerabilities, software stacks and bugs to exploit. For network managers, this means the costs of downtime and truck rolls are rising, new security paradigms are needed for workers accessing files from anywhere and there are simply more vulnerabilities that need to be monitored over greater distances.

With so many complexities piling up, organizations can greatly benefit from automated or AI-powered tools for crucial network functions like threat identification and recovery, low latency monitoring and provisioning and self-healing and management. These capabilities and more can easily be achieved on a console server or separate management plane that supports standard NetOps tools, such as Docker, Python, and Ansible,

By providing these tools on a separate management plane, organizations can rapidly recover from outages from any location and gain a bird’s eye view into all devices on a network. So, if someone ever tries to upload a virus via a USB drive in a remote location in the boonies or sends an army of malware links to your interns, you’ll be right there to prevent or stop it, no matter where you are physically.

Don’t wait, liberate

While a smart, separate network management plane significantly increases network resilience, many organizations haven’t adopted such an approach across their entire operations. For many, the technology’s value is not clear until it is needed in a crisis, or organizations may try to function with legacy out-of-band servers that are not scalable, rely on outdated firmware, or simply have limited capabilities.

But those who do keep using the primary network to manage the network or rely on outdated tools, may be in for a rude awakening. For those who act before it’s too late, though, a secure separate management plane may be the secret sauce needed to protect any organization seeking to capitalize on the emerging trends and technologies of today and into the future.

About the Author

Todd Rychecky is VP of Americas for Opengear, responsible for developing and executing sales strategies, business development initiatives, hiring and developing an award-winning sales team. For 13 consecutive years, Rychecky and his Opengear Sales teams have experienced year over year sales growth. He joined the company in 2008 and was the first sales and marketing hire, helping kick start Opengear. He has a wide range of experiences including sales, marketing, channel development, strategic accounts, OEM partnerships, and business development initiatives. His main focus today is on growing the sales teams, partner channels, and strategic accounts. Rychecky earned a bachelor’s degree from Nebraska Wesleyan University. He can be reached online at resilience@opengear.com, and at https://opengear.com/

How Supply Chains Should Protect Themselves from Data Breaches

By David Lukic, Security and Compliance Consultant at IDstrong.com

There has been a major supply chain breach in the last year. This was the now infamous SolarWinds hack. Many managers now wonder what they can do to defend themselves. The recommendation is to assume that a breach has already occurred. One should also utilize a defense-in-depth strategy to reduce vulnerability to attacks.

Supply Chain Attacks

Cybercriminals have become savvy to typical perimeter-focused defense strategies and are finding ways around them. One of these cunning methods of attack is called the supply chain attack.

This happens when the attack vector is hidden in something that has permitted access. Perhaps it has already infiltrated the permitted software, or perhaps it was intentionally attached. These threats can sneak through in software, software updates, service providers, or hardware.

The aforementioned SolarWinds hack is a great example of a supply chain attack. Late last year FireEye, a cybersecurity company, discovered and announced news of a cyber breach. FireEye was not, however, the first nor only company to fall victim to this attack.

Roughly 18,000 SolarWinds customers suffered after downloading a software update. This list includes multiple Fortune 500 companies and over 250 federal agencies. Damages include breached confidential data and data theft.

The original attack occurred long before this time. This was when the SolarWinds software was originally corrupted, but it went undetected. What makes this a supply chain attack is how the malware spread. It was distributed and installed by customers of the targeted company.

A Zero Approach

A zero approach, or zero-trust approach, is a security approach. It means that no software, hardware, person, or other potential threat carrier is trusted. It doesn't matter whether something comes from internal or external sources. Everyone and everything must be thoroughly checked before being allowed to access network resources. Nothing is privileged.

Without privileged parties, supply chain attacks are far less likely to succeed. Consider if the SolarWinds software update had undergone authentication procedures before being installed. The impact of the attack could potentially have been contained.

Ensuring that nothing is taken for granted may end up saving your business. The additional security of a zero approach could protect you from supply chain attacks. This could save your business from the likes of data breaches, and ransomware attacks.

Limiting Damage Post-Breach

It is important to attempt to contain the fallout as best as possible. One must, however, first assess the level of damage already done. Notify law enforcement if necessary, then engage in damage limitation. Limiting damage post-system breach can take shape through a number of strategies.

These measures include rerouting network traffic, filtering the attack, and isolating network components. The approach will differ based on the type of attack. Isolating all parts of a compromised network can prevent the infection from spreading. Filtering or blocking is often used with denial-of-service attacks, such as ransomware attacks.

If you find yourself in a ransomware attack, do not pay the ransom. One should be working against the cybercriminals, not with them. Work with law enforcement to discover the source of the attack and combat it.

Future Protection Trends

One trend to protect against data breaches is increasing the number of required security checks. This aims to decrease the chances of malware going unnoticed and corrupting data systems.

Increased integration of AI is another current trend to improve protection against cybercrime. AI is better able (than humans) to efficiently check for vulnerabilities in systems. It is also able to discover and respond to cyberattacks in under a second. In the case of the SolarWinds attack, millions of employees didn't even notice the attack for months.

Future Industry Trends

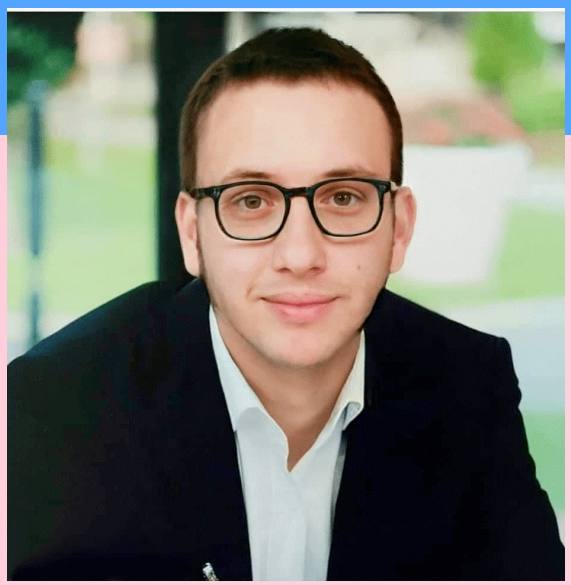
One key future industry trend is 'cyber threat intelligence'. Cyber threat intelligence helps people increase their understanding of the typical behavior of a cybercriminal. This means that they are better able to react appropriately and timeously to attacks.

An example of this is the institution of Cyber Fusion Centers, which takes a strategic approach to integrate technologies, processes, and teams. Even so, there are significant challenges to operationalizing intelligence in such a way that prioritizes activities for cyber defenders.

Businesses moving on to the 'cloud' is another popular trend in the industry. The popularity of this shift is well justified too. Using the cloud is far more efficient and more secure than traditional storage methods.

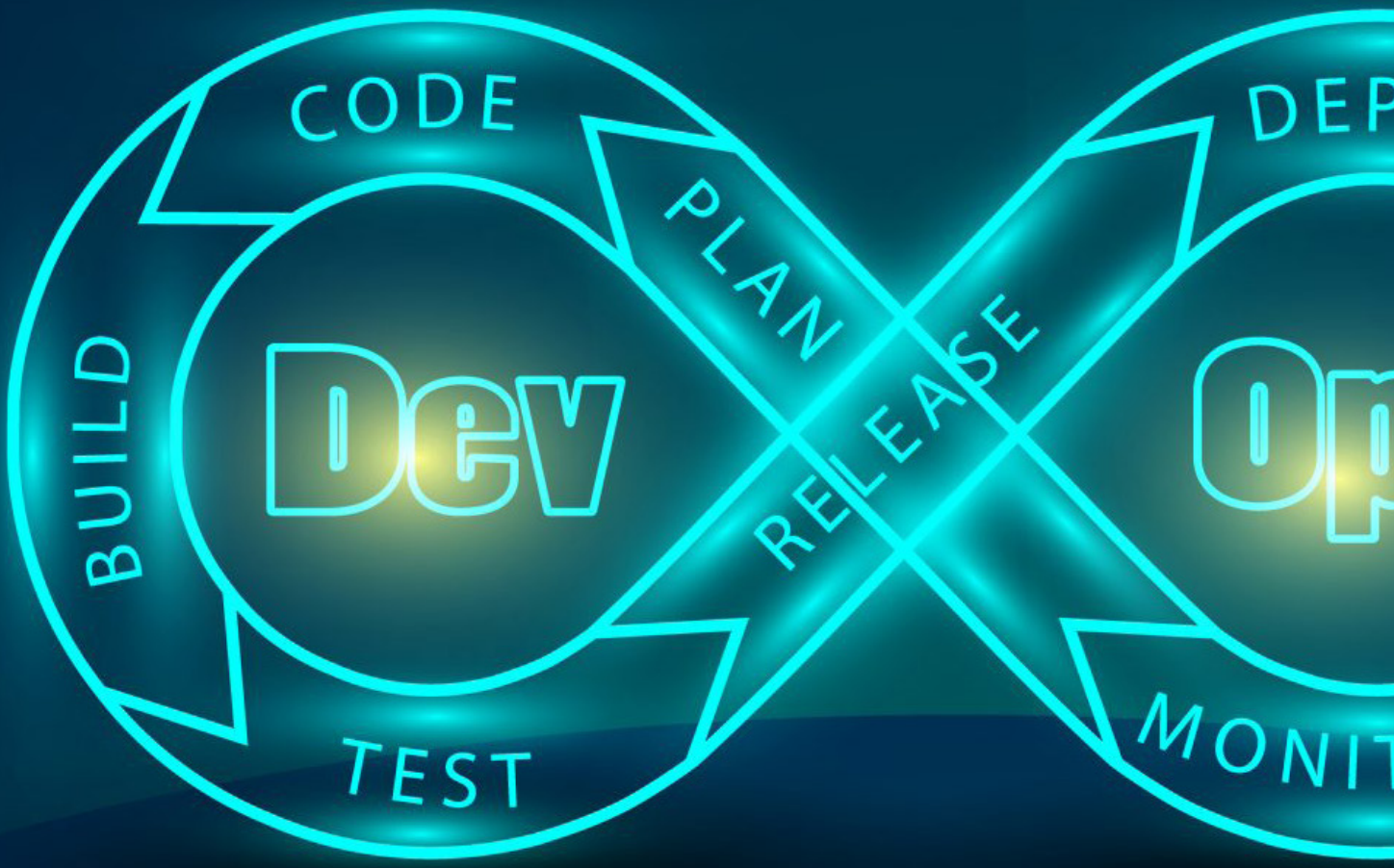
Supply chain attacks are a rising threat, with a high potential for serious consequences. Defense strategies are integral to the survival and safety of any business. Having a water-tight data protection plan is wise, especially in this current climate of ever-increasing cyber threats.

About the Author



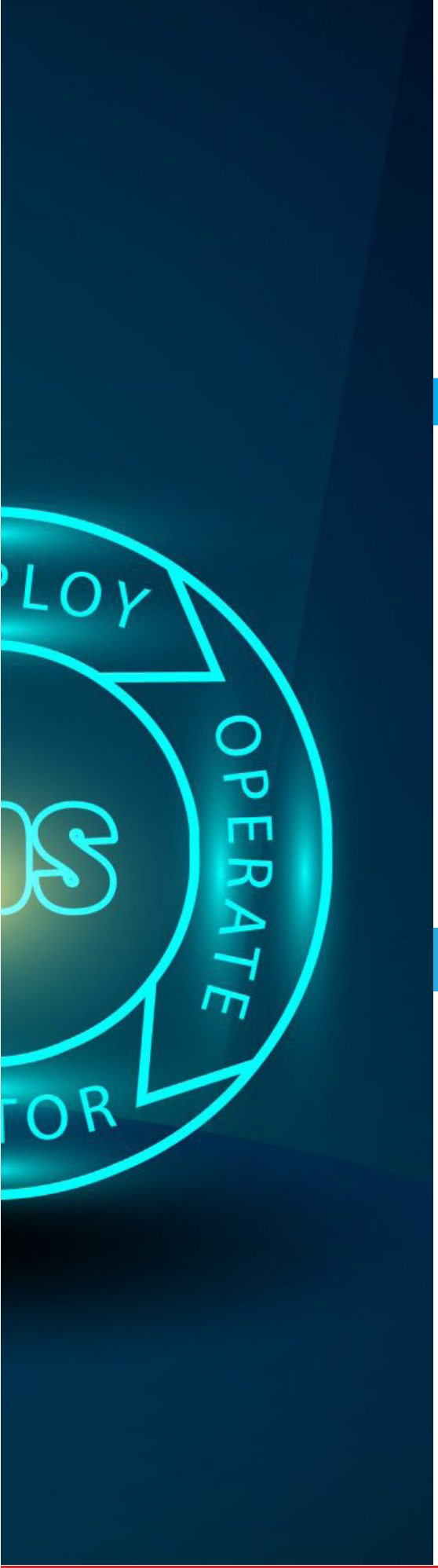
David Lukić is an information privacy, security and compliance consultant at IDstrong.com. The passion to make cyber security accessible and interesting has led David to share all the knowledge he has.

Learn more about him at https://www.idstrong.com/



DevOps Done Right With Infrastructure-as-Code Security

By Ulrica de Fort-Menares, VP of Product & Strategy, Indeni



With the advent of Infrastructure-as-Code (IaC), developers are provisioning cloud infrastructure and taking responsibility for infrastructure changes. This means developers have full control; owning the entire application stack along with the infrastructure stack. Essentially, IaC enables developers to achieve the goals for becoming more autonomous and agile. A developer can easily spin up a production-like cloud environment in a matter of minutes, both at scale and in a repeatable fashion. For many, IaC is a path to self-service IT empowering your developers to innovate at unprecedented speed.

Cloud Security Breaches Are Costly

While speed is of the essence inarguably, how do you ensure the cloud environment is secure? Do your developers have enough cloud security expertise that they are not bypassing certain security policies?

The 2020 Cost of a Data Breach report by the Ponemon Institute found that cloud misconfigurations were the most common causes of malicious breaches among organizations studied. According to the study, the average cost of a breach due to cloud misconfigurations was $4.41 million. Incidentally, Gartner also cited that there is more risk from cloud infrastructure misconfiguration than from workload compromise. Evidently, infrastructure security in the cloud is a serious matter; this makes the decision between speed and governance hard.

Why should you have to compromise speed for security, or vice versa? Is it possible to find the right balance between governance and speed?

Legacy Approaches to Security Programs Hinder Agile Delivery

The challenge is that security is often perceived as a drag on the required speed and agility of deployment. This is because legacy security programs happen too late in the development cycle. After the infrastructure is deployed, you tack on security scans at the end of the delivery process. If security issues are found, developers inevitably spend significant time and energy to investigate these security issues causing delay to the launch. The problem is exacerbated by the fact that these security issues often turn out to be false positives causing tremendous frustration to the developers. Uncovering issues that late into the cycle is expensive to fix, creating unnecessary stress and slowing delivery. All too often, organizations would end up opting for faster delivery by delaying security fixes at the expense of security.

Modernize your Security Programs with Shift Left IaC Security

The software development process has been shifting left to deliver software faster and with improved quality. The same should be done for the infrastructure with IaC security testing. By starting security testing early in the delivery pipeline, teams have more time to address them before pushing code into production.

Modern security programs should be fully automated and integrated into the DevOps pipeline. Full automation means that developers don't need to get in line for security reviews. Instead, IaC templates will be automatically evaluated for security impacts every time an infrastructure change or a new resource is about to be deployed. Developers will be alerted to the security issues relating to the infrastructure that need correction. Essentially, it's like putting guardrails in place to protect organizations from security risks in the cloud. Security risks can be instantly remediated at the time they are made allowing developers to move fast. You can think of the shift left security approach as testing IaC continuously and preventing insecure infrastructure from being deployed.

Best Practices for IaC Security

While it makes sense to integrate security controls at the beginning of the production pipeline, getting the developers community to adopt DevOps security requires more than just the right IaC security tools. Remember developers are always under relentless pressure to meet insane deadlines, any potential speedbump is considered a threat.

Top five best practices for IaC security:

1. Do not expect the developers to come outside their normal workflows. Instead, integrate your IaC security solution with the developers' workflows. Ideally, you want to bring IaC security into the tools that developers want to use and are already familiar with: Jenkins, GitLab, CircleCI, GitHub, JIRA, Slack, etc. Essentially a developer-centric security tool has a better chance to get adopted by developers.

2. Far too often security programs focus on the technology. Let's not forget that a successful DevOps transformation needs to bring people, process and technology together. On the people front, you want to empathize with the developer side in order to strike a balance between the developer and the security side of the house. Have a partner on the developer side to make joint decisions and reflect back on them. It is also important to establish common goals between developers and security teams. These shared goals must come from senior management. For example, when the production pipeline is halted, the security team must be part of the solution working alongside with the developers to resolve the security issues.

3. When you are ready to integrate your IaC security tool into the CI/CD, be sure the tool is in a learning mode. That means the tool cannot stop the pipeline just yet. The last thing you want is the tool stopping the CI/CD pipeline the moment it is implemented, negatively impacting the developers.

4. Once security tools are organically embedded into the development pipeline, you start to gain visibility into the cloud environment. Essentially, you have put security guardrails around your CI/CD process. You are now in a position to enforce security controls into the CI/CD pipeline with the intent to stop the pipeline upon detecting security violations. While the inclination might be to enforce the violated rules first in order to prevent the same risk from occurring, doing so would stop the pipeline. Instead, you should work with the developer to mitigate the problem and be part of the solution. Only until after the violation was resolved should you enforce the rule. You should always start with security controls that do not have violations, this way you don't impact the pipeline. In other words, you want your guardrails to be invisible during the initial implementation. By taking a pragmatic approach to implementing security controls, the IaC security solution would have a better chance to gain acceptance by the developers community.

5. A common critique of security testing tools is that they produce many false positives.
According to the ATARC (Advanced Technology Academic Research Center) Federal DevSecOps Landscape survey, too many false positives is the number one frustration with security testing. IaC security tools are no exception. A robust security tool needs to be doing more than just basic key-value analysis. For example, if a tool is flagging an AWS security group as a potential issue, it should check to see if the security group is in use, what subnet(s) it is used in, if there are firewall rules blocking access, are there Internet routes, etc. Essentially, the tool should employ the same logic a human would to determine if it is a real security risk before raising an issue. Without checking these conditions, you would almost certainly experience a lot of unnecessary noise. A noisy security tool can negate your security efforts, so be aware of this pitfall and pick an intelligent tool.

IaC Security is Essential to Your DevOps Journey

DevOps teams have the opportunity to "shift left" security processes in such a way without sacrificing speed. More importantly, the shift-left security approach is a new paradigm that is moving toward a preventive cloud security strategy. By integrating IaC security into the CI/CD pipeline, you can now take the appropriate preventive steps to remediate misconfigurations and security risks before they make it into your cloud environment. With IaC security, you can deploy fast while reducing the opportunity for exploitation by this shift.

About the Author

Ulrica de Fort-Menares is the Vice President of Product and Strategy at Indeni. Ulrica is responsible for the strategy, partnerships and execution of the Indeni product portfolio. With over 30 years of experience in the high-tech industry, she has held various leadership positions in product management, software development and network engineering. She is the holder of 7 patents in network technologies.

Ulrica can be reached online at https://www.linkedin.com/in/ulrica-de-fort-menares/ and at our company website https://indeni.com/about-indeni/

Cybercrime Case in Detail

By Milica D. Djekic

The majority of cybercrimes can happen if the hackers discover an IP address of the server or endpoint user. When that occurs there can appear a plenty of high-tech crime schemes such as DDoS, IT sabotage, espionage or the other ways of the cyber attacks. In such a case, it's significant thinking about safety and security of the potentially exploited IT resources. The fact is the hackers have skill and in their offensive to our assets they can choose so many tactics and strategies in order to take control over our IT infrastructure. For instance, it's possible to conduct the skillfully planned phishing operation and the needed IP address will be obtained.

Every single year the cybercrime costs the global economy trillions of dollars and for such a reason it's important investing into cyber defense. Also, there are a lot of social impacts that can embarrass the members of public if the web connectivity and our experience of the internet are not reliable enough. In addition, the main concern in the internet usage is that so many devices will be compromised, but no one will report about any incident. The reason for so is the majority of people are not

familiar with that how cybercrime looks like or in so many cases they will believe that no one will try to hack their private devices. Basically, that's the sword with two edges and if all the incidents would be reported straightforwardly we would recognize that the harm from high-tech crime is much bigger and indeed, there is the need to tackle such a challenge in much more serious manner.

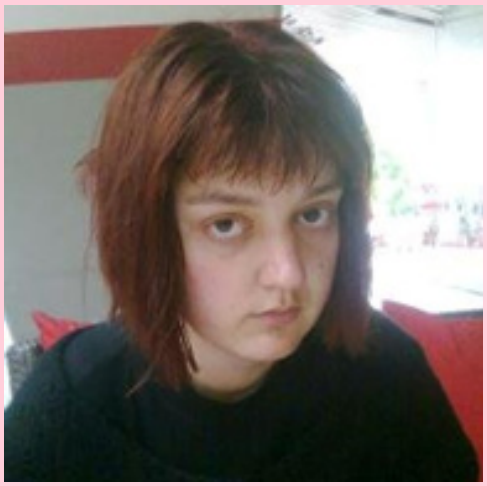
Apparently, any activity in the cyberspace will leave the footage and there is increasing need for the skillful cyber forensics that could investigate and document what happened in the virtual environment and their reports could serve as the evidence on the court in proving someone's guiltiness and intents, so far. In other words, anyone committing the cybercrime will also leave the trace and even if that person attempts to hide his IP address the trained forensic detectives can track that sort of the activity. The huge challenge is that in sense of the criminology the offenders need the reliable communication and they can get if their information exchange device emits the signal, so the surrounding telecommunication infrastructure is able to collect those findings and make their records in its memory storage. Indeed, anyone using the emerging technologies is not invisible and the experienced law enforcement staffs will know how to start the investigation.

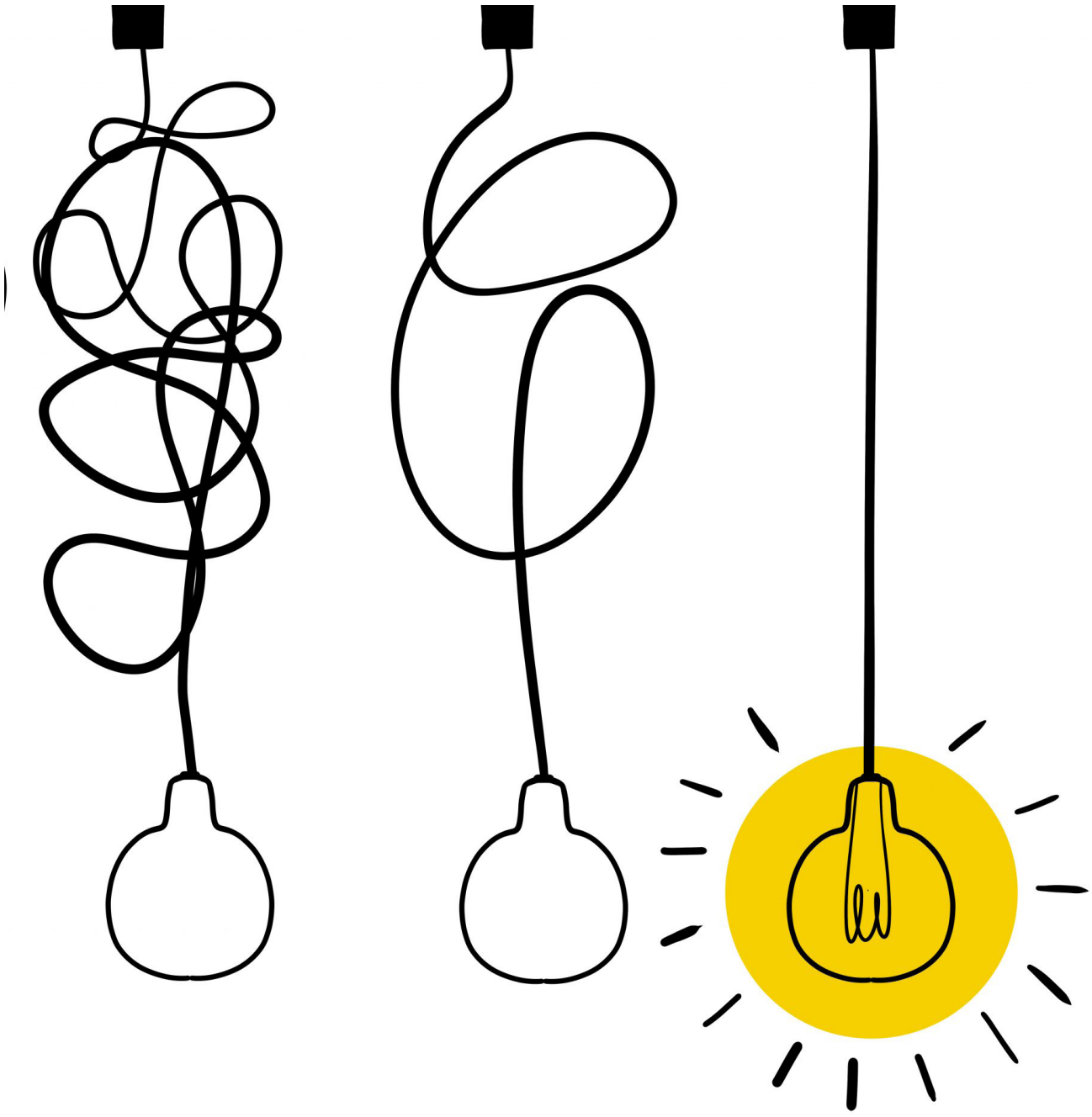
So, some criminal justice cases will rely on cyber systems and in such a fashion anyone willing to pay for the information will know that it is not smart taking the activated device on the crime scene. On the other hand, when the incident happens the investigation will firstly do some tracking on the crime scene and if the device is deactivated at that moment it could be hard to track such a route. Maybe the inspection will show that the criminals have undoubtedly been there at that piece of time, but we will not catch the signal – so it can seem that they used no devices at all.

As the bad guys have skill to commit their offenses the good case management is needed from the investigators and the other case members. Essentially, there are no the perfect crimes as there is no an absolute security so it's only the matter of time and effort when some security system or the criminal scheme can be broken and smashed once forever, so far.

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 book "The Internet of Things: Concept, Applications and Security" being published in 2017 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.





Need Cybersecurity Talent? It's Time to Get Resourceful

By Alex Hernandez, Vice President, Emerging Technology at DefenseStorm

Looking for a cybersecurity professional or two (or 100) for your organization? Join the club as companies worldwide face a shortage of IT security professionals that were already in scant supply before the pandemic and are now critically so. According to a survey by tech recruiter Harvey Nash and KPMG, more than one-third (35%) of companies are searching for cybersecurity professionals as their top priority. Further, 2020 was the first year in more than 10 that IT security skills topped the list of technology skills shortages, worldwide.

Since cybersecurity threats persist in a time when cybersecurity professionals are in such high demand, it's clear that companies are going to have to find creative ways to meet the need to protect themselves, their employees and their customers. Namely, they're going to have to look outside traditional criteria and rely more heavily on technology.

Digitization + Increased Attacks = Heightened Security Needs

Organizations worldwide are increasingly relying on digital initiatives: A McKinsey Global Survey of executives revealed that the pandemic brought about years of change in how professionals conduct business, regardless of sector. Further, respondents have accelerated digitization of their internal operations by three to four years. Thirty-seven percent of respondents also increased data security spending.

And it's no wonder when you consider damage done, for example, by the 2020 SolarWinds attack. Texas-based IT company SolarWinds provides network management systems to more than 300,000 clients; about 18,000 of whom downloaded updates affected by the supply chain attack embedded in SolarWinds's Orion Product. This enabled sophisticated hackers to obtain undetected access to a subset of affected enterprises for a minimum of nine months. The motivation behind the breach is unclear – as is the amount of damage done.

What is crystal clear, however, is the necessity for organizations to heighten their security measures. Yet with the need for cybersecurity on the rise, four million qualified employees are needed to adequately defend organizations. With a 0% unemployment rate in cybersecurity, opportunities abound for professionals with these skills. But there simply aren't enough of them. According to Wesley Simpson, chief operating officer of (ISC)2, a nonprofit organization that trains cyber professionals, "Unfortunately, the pipeline of security talent isn't where it needs to be to help curb the cybercrime epidemic. Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats."

From White Collar to New Collar

It's time to get crafty and think beyond looking for white collar cybersecurity professionals only. There's an innovative "new collar" approach underway that involves tapping cybersecurity professionals that might not have a traditional college degree but do have the requisite technical skills and aptitudes to fulfill the cybersecurity needs of many organizations.The new-collar approach focuses on skills that could have been honed through hands-on experience and professional certifications. For example, ex-military personnel are often great candidates to enter the cybersecurity professional workforce. Military veterans generally have soft skills like proactivity, analytical thinking and problem solving, and diligence to ensure work will continue unimpeded. All of which attribute nicely to defending a company's digital infrastructure. Consider the benefits of seeking, hiring and training candidates who have experience identifying and alleviating the impact of cyberattacks, or have specialized cloud security skills, for instance.

The Youth Movement Could Help

Think, too, of hiring younger professionals. The new-collar approach isn't the only novel idea that's been gaining ground in the past few years. Many organizations have been hiring up-and-coming talent because it can pay off in the future. By 2025, millennials will comprise 75% of the global labor force. Further, more than 70% of the ethical hacker community is younger than 30. Therefore, organizations should tap into this community – and Gen Z'ers, too – to build their cybersecurity workforce. Interestingly, the National Security Agency (N.S.A.) has been training kids to wipe out cybercriminals since 2014. Last summer, through a program called GenCyber, the N.S.A. ran 122 across-the-country cybersecurity camps called Camp Cryptobot, which were jointly funded by N.S.A and the National Science Foundation. The purpose of the free camps is to help generate interest in cybersecurity careers and generate a future pipeline of cyber workers. The Girl Scouts are also joining the cause: Security company Pala Alto Networks and the Girl Scouts of the USA joined efforts in 2017 to deliver the first-of-its kind Cybersecurity badge for girls in grades K-12. The message is loud and clear: to stem the cybersecurity shortage of today, companies need to look to, and possibly invest in, the cybersecurity professionals of tomorrow.

AI, ML and Hands-On Help, Too

And in the day of all-things digital, another method of tackling the skills gap is to invest more heavily in technology that includes artificial intelligence (AI), machine learning (ML) and behavioral analytics. ML supports things like behavioral analytics and detects threats buried inside interrelated data. AI discovers threats and delivers insights into their origins. In fact, AI-powered security technology can help organizations improve their security posture by detecting ongoing or impending attacks, especially when security personnel are scarce or overburdened. However, relying too much on ML and AI can create a false sense of security. This is why some organizations reach out to external experienced professionals for help. For instance, some cybersecurity solutions offer a hands-on team that virtually monitors security alerts around the clock to provide a human element to an automated process. Others rely on a security operations center (SOC) to monitor and analyze their security posture and respond to cybersecurity incidents on their behalf.

Creativity is Needed to Bridge the Talent Gap

The ongoing and increasing cybersecurity skills shortage leaves room for untold vulnerabilities. Companies worldwide are four million cybersecurity professionals shy of filling the positions they need. Until then, it's time to think outside the box. Cybercriminals are always upping their game, so organizations must do the same.

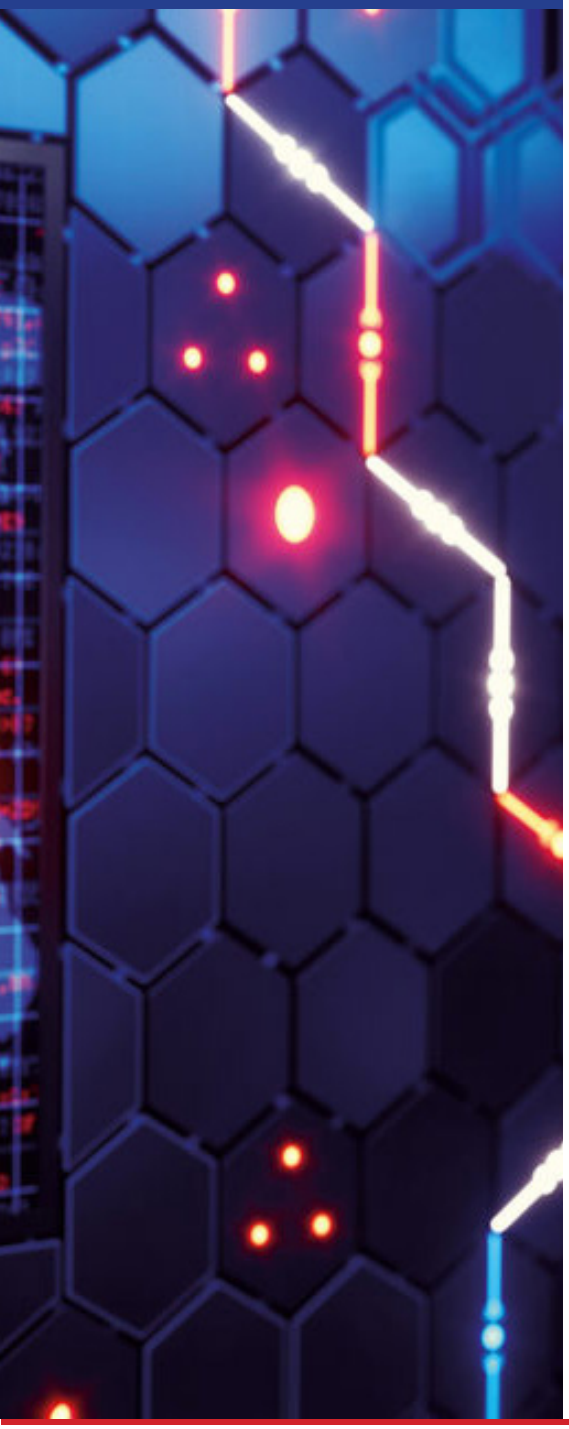
About the Author

Alex Hernandez,Vice President, Emerging Technology.Alex has more than 20 years of experience providing security solutions and expertise to some of the largest companies in the world. He regularly speaks at regional and national IT and security conferences, and frequently is a featured expert at cybersecurity association meetings around the country. Alex has worked with several leading security solutions providers, including Barracuda Networks, Purewire, Secure Computing, CipherTrust, S1 and SecureWare. Alex holds a Bachelor of Science degree in Computer Engineering from the University of Florida.

Alex can be reached online at @the_hern on Twitter and at our company website https://www.defensestorm.com/

Six Insidious Cyber Attacks that Impacted the Industry in 2020

By Eyal Gruner, Co-founder & CEO, Cynet



2020 was the year that COVID-19 brought a major cyber-pandemic to the world. An assessment by INTERPOL revealed that organizations and businesses rapidly deploying remote systems and networks to support staff working from home were being taken advantage of by cybercriminals. The report noted that in a four-month period, "some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs – all related to COVID-19 – were detected by INTERPOL and its private sector partners." Many of these never made the headlines, but six major attacks did – ranked below by their overall impact.

Today, we turn back the pages of 2020 to review the most noteworthy cyberattacks making up the cyber-pandemic, which came with COVID-19 and the flight of employees to remote work environments. These cyber events were part of an ongoing series of attacks, keeping IT security professionals on high alert.

1. **The SolarWinds Attack -** This attack involved hackers compromising the infrastructure of SolarWinds, a company that produces a network and application monitoring platform called Orion, and then using that access to produce and distribute trojanized updates to the software's users.

2. **FireEye: The Stolen Red Team Tools -** On August 12, 2020 FireEye announced that a sophisticated group of hackers, likely state-sponsored, broke into its network and stole tools that the company's experts developed to simulate real attackers and test the security of its customers. The attack was later found to be tied to SUNBURST malware which was also responsible for the SolarWinds attack.

3. **Software AG: Clop Ransomware Attack -** The second-largest software vendor in Germany was reportedly hit by a ransomware attack in October 2020. News outlets reported that the German tech firm had been attacked by the Clop ransomware and that the cyber-criminal gang had demanded a $23 million ransom.

4. **Sopra Steria: Ryuk Ransomware Attack –** The 46,000 employee European information technology firm announced on October 21, 2020 that it had detected a cyber attack the previous evening. The virus was identified as a new version of the Ryuk ransomware, previously unknown to antivirus software providers and security agencies. The attack followed a previous infection with either TrickBot or BazarLoader.

[1]INTERPOL, INTERPOL report shows alarming rate of cyber-attacks during COVID-19, August, 2020

5. **Telegram Hijack –** Hackers with access to the Signaling System 7 (SS7) used for connecting mobile networks across the world were able to gain access to Telegram messenger and email data of high-profile individuals in the cryptocurrency business. In what is believed to be a targeted attack, the hackers were after two-factor authentication (2FA) login codes delivered over the short messaging system of the victim's mobile phone provider.

6. **BlackBaud: Ransomware Attack** - Blackbaud, a cloud technology company, was hit by a data-stealing ransomware attack earlier this year. The attack was one of the biggest of the year in terms of the number of organizations affected, with nearly 200 organizations and millions of individuals potentially impacted.

Lessons Learned

The most common causes of data breaches are weak or stolen credentials, back doors/vulnerabilities, malware, social engineering, excessive permissions, insider threats and improper configuration/user error, so businesses need to be diligent. Cybersecurity needs to be top of mind and systems and setups need to be routinely assessed. Any organization can become the victim of phishing schemes, ransomware, DDoS, malware, and other attacks leading to data breaches. Stress to customers that taking all necessary precautions is the best chance they have at staying secure. Along with detection and response tools, authentication protocols and ongoing employee security awareness training can make the biggest difference.

Because the reality is challenging and the future is not promising to be better in terms of cybersecurity threats and malicious attacks, cybersecurity pros must be prepared in the defense of their organization. Going deeper into 2021, organizations are more prepared than ever to address these challenges and improve overall security readiness with technologies such as next-generation XDR (EPP, NGAV, EDR, NDR, UBA), SOAR and advanced MDR services.

About the Author

Eyal Gruner is the co-founder and CEO of Cynet. He is also co-founder and former CEO of BugSec, Israel's leading cyber consultancy, and Versafe, acquired by F5 Networks. Gruner began his career at age 15 by hacking into his bank's ATM to show the weakness of their security, and has since been recognized in Google's security Hall of Fame. Eyal can be reached online at @Cynet360 and at our company website http://www.cynet.com.

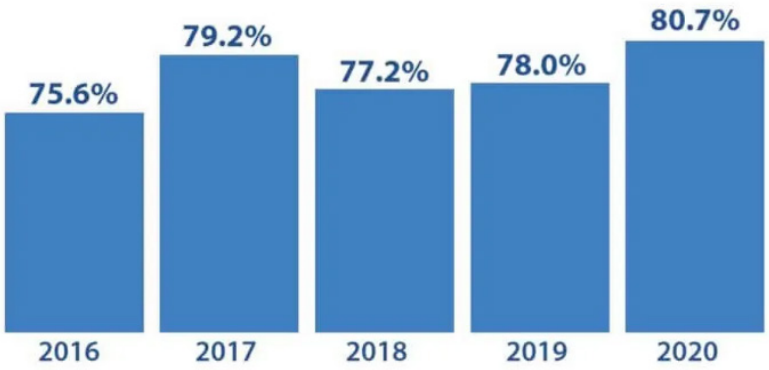
Why Threat Intelligence Matters Now More Than Ever:Cyber Threat Intel Is the Need of The Hour

By Leo J Cole, CMO, Futurism Technologies, Inc.

The menace of cyber attacks and data breaches have become increasingly common, as business around the world wake up to the idea of remote working since the outbreak of COVID-19. Yes, the pandemic has pushed many brick and mortar businesses into a black hole type situation with immature security and IT tools and processes leaving them vulnerable to attacks.

According to a report on cybersecurity breaches, more than 40% of businesses experienced a security breach between Q2 2019 and Q2 2020 with an average breach attempt made every week. In another report by IBM, it was found that the average cost of a security breach is anywhere around USD 3.86 million with healthcare being the most affected. The report also revealed a startling finding i.e. it took an average of 280 days to detect and contain such a breach.

The pandemic provided the bad actors with a rapidly burgeoning corporate attack surface to exploit and carry out network and system breaches. These attacks grew by leaps and bounds as businesses try to bounce back in the post pandemic world. The sophistication of SolarWinds attack took everyone by surprise with the attack going undetected for so long.



RISE IN ATTACKS EVERY YEAR
(CREDIT: CYBEREDGE GROUP 2020 CYBERTHREAT DEFENSE REPORT)

Why threat intelligence has become the need of the hour

Attackers are tailoring world-class exploitation capabilities to target network and security systems. Such breaches unlock a hotbed of opportunities for cybersecurity professionals to reevaluate every aspect of their security strategy including people, processes, threat detection rules, tools and research methodologies. Today, without a comprehensive threat intelligence model, it is more like a fire dousing effort than a preventive effort. This is why businesses ought to wake up to the idea of cyber threat intelligence. In fact, threat intelligence has to sit at the core of an organization's overall cybersecurity strategy to keep such sophisticated breaches and attacks at bay.

"In addition to preventing network attacks that expose businesses to intellectual property, monetary and compliance related risks, threat intelligence also gives the organization a bird's eye view of its security teams overlooking sophisticated attacks that may take place through emails, social media, enterprise/mobile applications, etc.," said Mr. Sheetal Pansare, President & Global CEO for Futurism Technologies, Inc., a leading and global digital transformation advisor and consulting partner.

Unfortunately, organizations and security leaders often get confused between cyber threat information and cyber threat intelligence.

Threat Information vs. Threat Intelligence

Threat Information	Threat Intelligence
• Unstructured, raw data/feed	• Structured, sorted information
• Often unevaluated	• Well-evaluated
• Aggregated from multiple sources	• Aggregated from reliable sources
• Not actionable	• Actionable

A threat intelligence model helps a business to proactively prevent, identify and remediate data breaches and is a boon in reducing the cost of a security breach. Threat intelligence comprises of various key tools to make sure that your business is well-equipped to drastically reduce the damage in the event of an attack.

- Threat intelligence plays a pivotal role in understanding various threat actors, campaign patterns Common Vulnerabilities and Exposures (CVE) and Tactics, Techniques, and Procedures (TTPs) helping organizations paint a picture of the evolving threat landscape.
- It helps SOC teams to foresee specific patterns and attacks and prepare accordingly.
- It offers valuable insights into the security loopholes while offering the quintessential intel required for swift remediation.
- It provides security teams with actionable intel pertaining to leaked credentials.
- It also provides the ability to intercept stolen credential information, as it traverses from malware-infected systems/users or networks to the crime servers ensuring proactive defense system.
- Helps in proactive threat monitoring helping businesses to detect external risks in real time allowing them to root out threats before they occur.
- Threat intel obtained from reliable cyber communities provides the organizations with powerful insights into the tactics, methods and motivations of various threat actors.
- Threat intelligence also helps businesses to comply with regulatory and legal requirements. This can be evaluating a company's data processing capabilities or adhering to a risk-based approach to their security practices such as EU's NIS protocol, GDPR, etc.
- Threat intelligence not only reduces the cost and risks associated with a data/security breach, but also helps a business to align and prioritize its security spending with its requirements.
- Threat intelligence improves an organization's overall security posture by significantly reducing the incident response time.
- Helps to proactively identify threats in a faster manner, reduce events and incidents significantly
- Accelerates threat investigation process and helps with situational awareness and reporting

The 'Why' matters more now

Not all businesses employ a huge cybersecurity unit or team that is armed with the required tools to uncover threat intel. This is where it counts to have a managed security service vendor by your side to keep up with evolving threat actors and sophisticated attacks.

It is pointless if you are attacked only to found about it a year later! This calls for having an advanced cyber threat intelligence detection and emergency incident response model or mechanism in place to identify, detect and respond.

A reliable managed security service provider can provide round the clock security by leveraging advanced cyber threat intelligence tools such as WAF (Web Application Firewall), firewall intrusion prevention systems, and other toolkits to help you monitor and protect your digital assets and endpoints efficiently.

Threat intelligence is being increasingly adopted by companies around the world to manage and tame the cost and risks associated with a breach or attack before it turns ugly. Data breach is every company's worst nightmare. Rather than distressing about it, businesses ought to reassess their security infrastructure and leverage the power of threat intelligence to secure their assets from various threat actors out there.

About the Author

Leo J Cole is the CMO at Futurism Technologies, Inc. With an industry experience spanning over three decades, Leo is a subject matter expert in Enterprise Software and Service, Security and Managed Services. An ardent cyber security evangelist, Leo has had many speaking engagements including AHA's Leadership Virtual Conference and was also featured on CNBC. You can find Leo on LinkedIn and our company website https://www.futurismtechnologies.com/

Protecting the COVID-19 Vaccine from Bad Online Actors

By Ksenia Coffman, Product Marketing Manager, NETSCOUT

The world breathed a sigh of relief when the first COVID-19 vaccines were approved for emergency use. But not everything is going smoothly. There is a lot of confusion about vaccine distribution and administration, with contradictory statements from public officials. Eligibility and scheduling also vary among states and counties. And with "anti-vaxxers" proliferating online, there are fears that certain population segments will refuse the vaccine altogether if they do not know who to believe.

As a result, governments need to conduct public education campaigns that prioritize accurate information. At the same time, they must coordinate large-scale, logistically challenging vaccination drives. Those dueling priorities often result in chaos.

Hackers watch these news cycles just like everyone else. Both good news and bad news give them ample opportunity to take advantage of peoples' vulnerability or generosity. The environment is ripe for disinformation and cyberattacks, which means phishing or malware campaigns could target specific medical providers or even the general population. Vaccine-related intellectual property is also highly valuable, so pharma companies are easy targets.

While physical security to protect against theft or intentional mishandling is still vital, in-depth cybersecurity strategies are essential to protect trade secrets, patents, clinical trial data, supply paths, and development and manufacturing agreements.

Medical providers must identify the eligible individuals in every vaccination tier to ensure equitable, efficient, and speedy distribution. Since many vaccines require two doses for full efficacy, public health authorities need to retain accurate data on which individuals already received shots from which manufacturers and ensure they get the correct second dose.

Countries employing so-called "vaccine passports" as part of the reopening process also possess a treasure trove of privacy-sensitive information. They need a thorough account of which individuals, private entities, and government authorities can access this data.

Ensuring total and pervasive visibility into this potentially overwhelming volume of vaccine information is critical to secure it, so the expected guardian does not become an unwilling sieve to extract or adulterate information.

Behind the scenes, industry-proven management systems should share the same underlying packet data, allowing network and operations teams to make decisions in concert. These tools need to facilitate quick detection, investigation, and response to threats while making it easy to integrate with security information and event management (SIEM) platforms.

Hybrid cloud approaches are best because they integrate traditional network architectures in a physical data center. That way, healthcare IT professionals will retain visibility as they migrate to the cloud or roll out native applications. Tools with agentless packet access and cloud-resident virtual instrumentation add minimal load to any cloud infrastructure.

But gaining a pervasive view is only the beginning. It is increasingly difficult for cybersecurity teams to rely solely upon log-based data for threat detection, investigation, and remediation. Industry professionals realize that wire-based metadata and packets contain the single source of truth. Whether securing an internal corporate network, remote office location, or cloud environment, medical enterprises and public health authorities need an intelligent retrieval system that investigates and remediates breaches quickly.

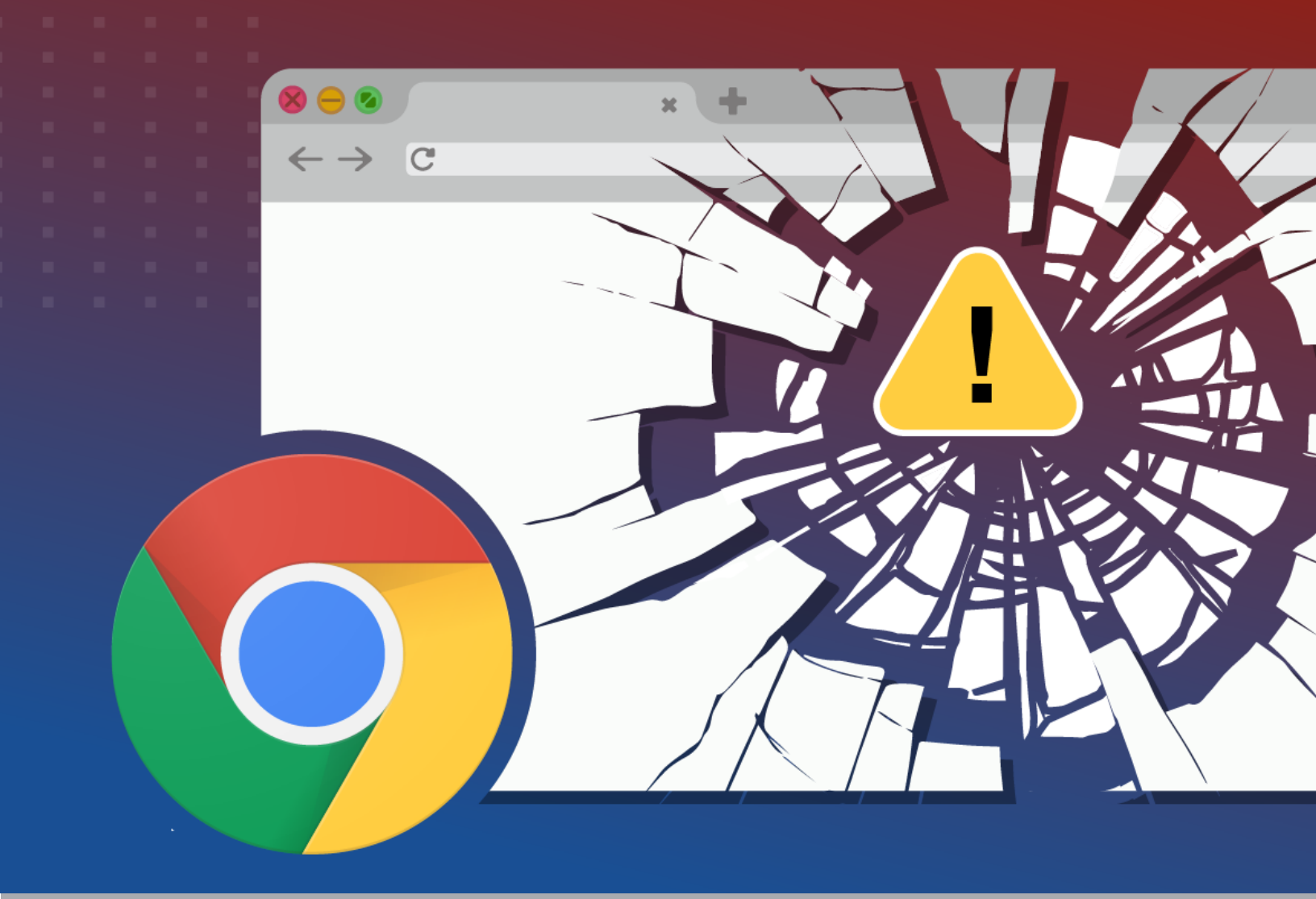
Adding contextual, real-time analytics and threat intelligence allows users to turn massive amounts of wire data into actionable insights for efficient cyber-threat detection and investigation. Agencies should conduct host and network investigations simultaneously. The former provides visibility into internal and external host interactions, while the latter offers a 360-degree view of servers,
applications, and conversations. Both crucial elements require packet stores for critical data and centralized indexing to enable fast retrieval and analysis.

Speed of execution, coordination among various agencies, and data protection will be critical to make the COVID-19 vaccine rollout a success. In the current environment of fear and uncertainty around vaccinations, there is no time to waste.

About the Author

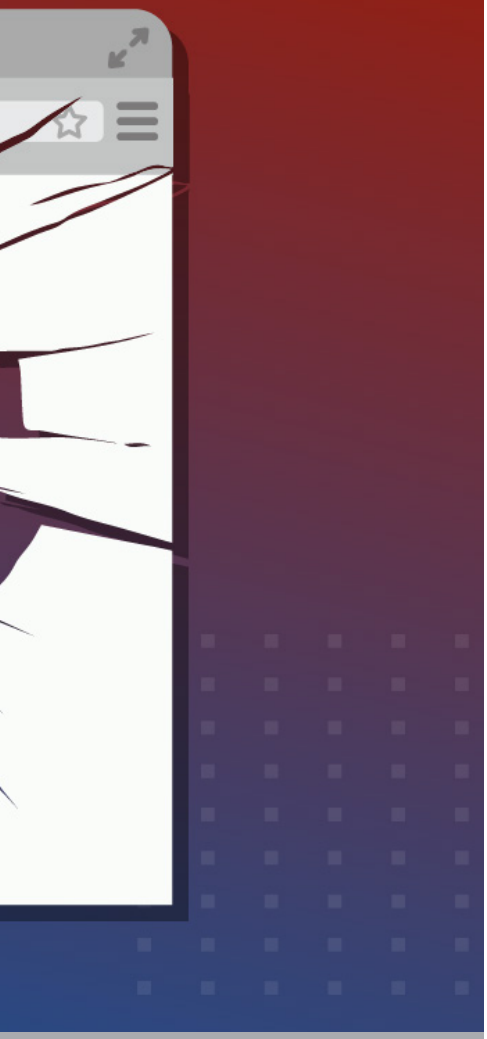
Ksenia Coffman, Product Marketing Manager at NETSCOUT, is a seasoned professional in the areas of security, networking and wireless. She has worked at NETSCOUT for the past five years, and previously held similar roles at companies such as AirTight Networks, Firetide, and Spirent Communications.

Learn more about her at https://www.netscout.com/



Chrome Browsers, Zero Day Attacks and the Impact of Patch Lag

By Vinay Pidathala, Director, Security Research at Menlo Security



Last year was a challenging year for organisations for a number of reasons. Perhaps one of the biggest for businesses is the shift to homeworking on a huge scale. This shift to remote working and increasingly to the cloud has resulted in a larger attack surface area that cyber criminals have capitalized on.

In 2020 we saw a resurgence of ransomware attacks and an increase in credential phishing campaigns, as well as new and novel attacks targeting cloud assets and resources. Browsers in particular have become even more tempting and are being used to access new applications and cloud services.

Since the first browsers arrived in the 1990s, they have been a target for malicious actors. As they have continued to evolve, so too have the ways hackers exploit their vulnerabilities. In the past, attackers could exploit a security flaw in a minor feature and spread laterally throughout the software stack. Now, once they get in, they have to find ways to move – either by trying to access the core OS of the device or by hijacking the browser process. This requires finding and taking advantage of bugs at different levels of the OS, the browser, and the browser functionality.

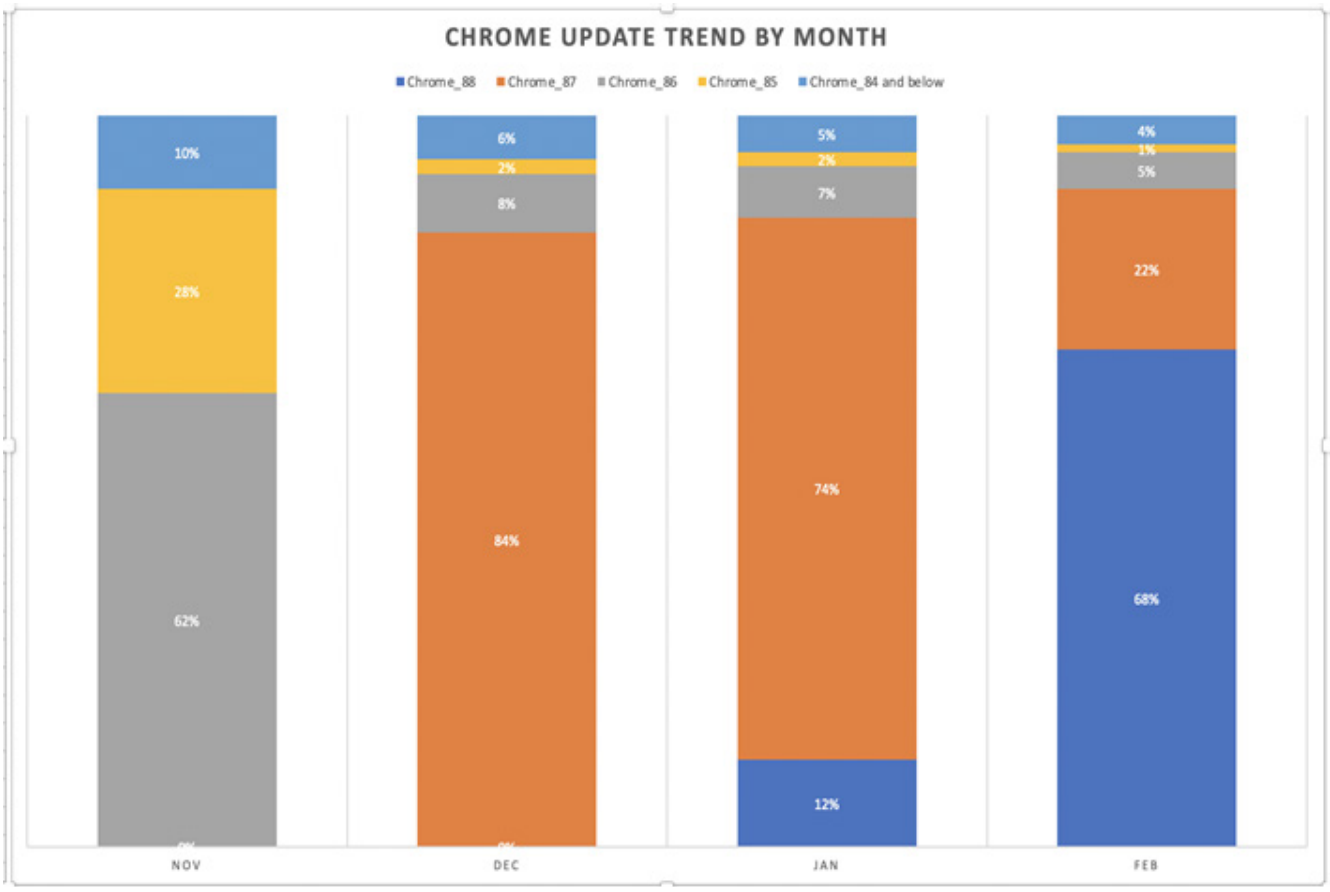
While we continue to see new and novel types of attacks, one technique that has persisted is the use of web browser exploits to compromise endpoint systems. Although we don't see a lot of exploit kits these days, we are seeing more sophisticated attacks that continue to use this infection vector by developing zero days.

Of the zero days that attackers have actively exploited in the wild during last year, there's a clear shift in attackers developing more zero days for Chrome. But why is this? For a start, Chrome has the largest market share, so it's natural that attackers will go after it – and this will only increase in the future. In addition, starting in January 2020, Microsoft's Edge browser became based on Chromium. Developing an exploit for Chrome now gives attackers a much larger attack surface to go after.

After Google fixed five flaws in Chrome in a span of a month, Menlo Labs published a blog at the end of last year revealing that a number of customers were still running old versions of the browser. In fact, 83% were still running versions of Chrome that were vulnerable.

Looking at the Chrome browser update cycle across the Menlo Security global customer base, we can see this 'patch lag' – the time between a new patch being made available and users installing it.

The graph below shows data collected from our global platform over four months, November 2020 to February 2021. It clearly shows the adoption of Chrome updates after they are released. For context, the release dates of the Chrome versions in the chart below are: Chrome 88 on 19 January 2021; Chrome 87 on 17 November 2020; and Chrome 86 on 6 October 2020.



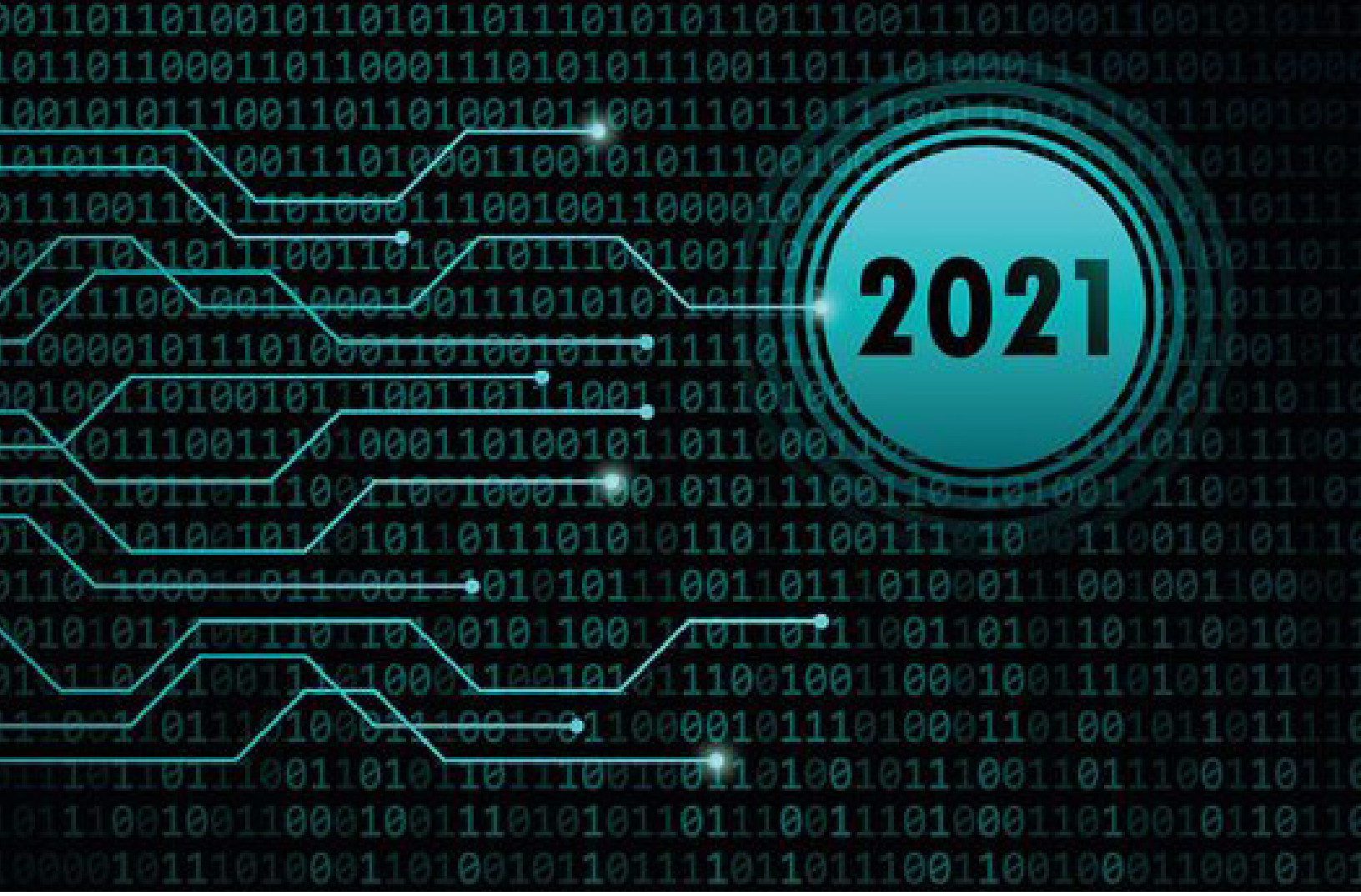
We can see that while Chrome 87 was released on 17 November, it took at least a month for customers to start updating their browsers. It was only in December that we saw Chrome 87 adoption rates of around 84%. We then saw a similar trend going into January of this year. Chrome 88 was released on 19 January 2021, and there was a significant increase in Chrome updates, with 68% of customers updating it by February. This quicker adoption could be attributed to the recent SolarWinds breach, with customers being more vigilant with updates.

According to our Threat Labs research, we also noticed that there were some early adopters of browser updates and those who were more consistent in their patching cycle. The same set of customers who were early adopters of Chrome 87, also updated more quickly to Chrome 88.

These early adopters included organisations in Finance & Banking,Government, Construction and Oil & Gas, while North America and
Singapore had the most customers updating as soon as the patch was released.
With the market dominance of Chrome, organisations must rethink their patch management policies in order to stay ahead of browser attacks. The need to patch as soon as possible is critically important. But for businesses unable to install patches immediately, a patch buffer can help mitigate attacks by providing them with the time they need to implement patches across multiple devices and keep users safe.

About the Author

Vinay Pidathala, Director of Security Research,Menlo Security. Vinay Pidathala is Director, Security Research at Menlo Security based in Mountain View, California.
Previously, Vinay was at Aruba Networks and also held positions at FireEye and Qualys.
Vinay can be reached online via our company website: https://www.menlosecurity.com/



Cybersecurity Trends to Watch in 2021

By Bob Blakley, Operating Partner, Team8

The pandemic accelerated the rate of digital transformation, driving faster uptake of cybertechnologies and creating a larger threat surface and more opportunities for attackers. As the threat surface increased, so did security budgets, with 57% of CISOs saying their security budgets increased this year, according to our 2021 Team8 CISO Survey.

Through conversations between Team8 cybersecurity experts and our CISO Village – a community of 350+ C-level security executives from 300 enterprises – we've identified the top areas we believe will be of critical importance to the cybersecurity industry over the next few years. We also included our unique perspective on how attackers think and operate, as well as the Team8 2021 CISO Survey and other internal resources, to develop our findings.

Looking into 2021 and beyond, here are our top trends for the cybersecurity industry:

1. Cloud Security

2020 was a pivotal year for cloud adoption as businesses sought to extend employee IT service access beyond the walls of the business, cut costs, retain flexibility, and throttle demand due to dislocation caused by the pandemic. According to the Team8 survey, cloud security (64%) is the number one investment area for 2021, followed by security automation (53%) and identity and access management (52%).

Cloud is now becoming so complex that it should be perceived as an operating system. Rather than applying legacy solutions to the cloud, organizations need security solutions that are architected for the cloud, combining control and integrity with scalability and agility.

2. Security of Things

2020 saw an explosion of connected devices. While new devices are coming online, old technologies, including manufacturing, remain vulnerable.

Legacy systems are continuing to be connected to the internet, as are Industrial IoT (IIoT) technologies. IT/OT convergence has the ability to unlock tremendous business value, leading to improvements in operational efficiency, performance and quality of service. Yet, new threat types expose the need for better endpoint defense. Novel attack patterns and approaches are cropping up every day that require a shift from signature-based detection to more advanced and dynamic behavioral-based techniques. Enterprise security teams simply can't stop them all, and a lack of asset visibility and management and security updates compounds the problem.

The shift in ransomware from focusing on data and IT infrastructure to disrupting OT environments is accelerating and is now one of the greatest threats facing CISOs and CIOs today. To mitigate risk of threats that cross the IT/OT boundary, new models and mindsets are needed.

3. Perimeter-less World

Remote-first work will remain with us in a post-pandemic environment, with 72% of office workers indicating a desire to retain the flexibility to work remotely. The global workforce has become reliant on at-home Wi-Fi networks, non-hardened work devices, and online collaboration tools – all trends which accelerated during 2020's pandemic-enforced remote-work period. Organizations must quickly move beyond perimeter-based solutions to secure the growing number of applications and resources hosted in the cloud, available as a service, and on mobile systems.

4. Privacy & Digital Trust

Many organizations have a hard time keeping up with ever-changing regulations because they lack an effective Governance Risk and Compliance (GRC) program, and regulations often conflict with one another, making it costly and complicated to comply. To improve compliance and earn consumer confidence, organizations need to take a proactive approach with tools, systems and services that help them get ahead of business risk by managing personal information within their enterprises and the supply chain, respecting regional variations in data regulations and transparently supporting consumers' instructions about data sharing.

In the future, the use of personal data may be controlled by the individual to whom the data refers, which will drive changes in business models, regulations and security.

5. Resilience & Recovery

Ransomware and destructive malware are on the rise. Enterprises are adjusting to business disruptions caused by the pandemic, making disaster recovery and business continuity plans essential. Network outages can impact businesses for months. Companies need to develop their "Plan B" and be prepared with a reboot plan designed for the digital age.

6. Shift-Left

Time to market is often prioritized over security. Developers are measured by how fast they can code, rather than on how securely. With no time to fix insecure code at the source, security is often "bolted on" once an application is fully developed – a risky approach. According to Forrester, 42% of organizations that experienced an external attack blamed the incident on a software security flaw, and 35% blamed a buggy web application. In today's environment of micro-releases and daily or weekly software updates, software developers need to maintain a security mindset and rely on controls throughout the coding process.

Despite this, the migration to a developer-driven security paradigm has been slow; Google reports that only 20% of firms are considered "elite performers" with DevOps. "Shift-left" highlights the need for security teams to work with developers from the very beginning of the development lifecycle to build in information security and security automation. Ideally, developers are empowered to embed security while creating a product or service, with tools that not only make code more secure but also codify intent. Security pros should develop their coding skills, and developers need to have the training and tools to code with security in mind.

7. Smarter Security

With organizations deploying and managing more security tools to manage their expanding networks, CISOs are being bombarded by vendors with tools that solve specific problems but that don't interoperate. The tools also have hidden costs associated with managing the data and tying it all together to create actionable insights. The shortage of skilled cyber talent exacerbates the problem. Enterprises need smarter security that leverages automation, data and AI so that humans can focus on decision making.

We are entering a new age for the cybersecurity industry. As companies accelerate their digital transformation, systems become more complex and expansive, and attacks become more frequent. This historic shift will set the stage for the next cybersecurity cycle and the generation of companies it develops.

About the Author

Bob Blakley is an Operating Partner at Team8. He was previously Global Director of Information Security Innovation at Citi. He recently served as a member of the National Academy of Science's Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing. He has also served as Plenary chair of the NSTIC Identity Ecosystem Steering Group and as Research and Development Co-Chair of FSSCC – the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. He is currently a member of the Forum on Cyber Resilience – a National Academies Roundtable.

Prior to joining Citi, Bob was Distinguished Analyst and Agenda Manager for Identity and Privacy at Gartner and Burton group. Before that, he was Chief Scientist for Security and Privacy at IBM. He is past general chair of the IEEE Security and Privacy Symposium and the ACSA New Security Paradigms workshop. He was awarded ACSAC's Distinguished Security Practitioner award in 2002, and is a frequent speaker at information security and computer industry events.

Bob received the A.B. in Classics from Princeton University, and the MS and PhD in Computer and Communications Science from the University of Michigan.

Bob Blakley can be reached online at @bobblakley and at our company website https://team8.vc/

Do You Trust Your VPN? What to Consider Before Installing VPNs For Security

By Brad Ree, CTO, ioXt Alliance

Virtual private networks (VPNs) are an integral part of many organizations' security framework to ensure that private information remains secure within their networks. Since the beginning of the pandemic, there has been an increased need for VPNs to accommodate employees continuing to work from home - in fact, according to a Top10VPN report, VPN demand was over a third higher than average during the first months of the pandemic, demonstrating how essential VPNs and security are to companies.

There are few services that can compete with the capabilities of a VPN, which provide users with end-to-end encryption of data, anonymized online activity and traffic, and the ability to securely connect to networks – especially public networks. VPNs also allow users to hide their locations, providing a level of privacy so no one can track where they are going, or coming from, and the content that is being looked at, which ultimately prevents hackers from spying and exploiting information from employees. Despite how its services are advertised, there currently lacks a reliable way to test VPN security before it hits the market, which has led to a number of vulnerabilities left unchecked for hackers to take advantage of.

In August 2020, the Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency released a cybersecurity advisory to bring attention to a vishing campaign that was executed through misleading VPN logins. Hackers registered domains and created phishing pages by duplicating a company's internal VPN login page - even capturing the two-factor authentication (2FA) and one-time passwords (OTP) needed to log in. From there, the cybercriminals posed as members of an employee's IT department and convinced the targeted employee that a new VPN link would be sent that required their login. Once the employee logged in, the hacker recorded the credentials and used it in real-time to gain access to corporate tools and company information using the employee's account.

With the absence of global security standards for VPNs, these types of attacks are made possible, leaving end-users exposed, even when they thought they were safe. With more companies looking to use VPNs as employees continue working from home, how can they ensure that the VPN is trustworthy and that their private information remains secure?

VPN Security Oversights

VPNs have two core promises – to create secure pathways for data and keep user information safe – which is what makes them appealing to companies, especially those working from home. However, many VPN services fail to abide by these promises and provide little transparency to users, leaving openings for hackers to exploit and breaking down the trust of everyone using the service. This can be seen with the Zyxel vulnerability, where more than 100,000 Zyxel firewalls, VPN gateways, and access point controllers contained admin-level backdoor accounts, allowing hackers access to devices and companies' networks.

Additionally, after installing a VPN on a device, employees might find it challenging to determine if their private network is connected, and remaining connected while in use. This is because there is a lack of visibility and visual cues, which creates consumer uncertainty on if they are actually browsing securely. To remedy this issue, VPN providers should ensure that their services are connecting automatically to prevent unwanted disconnections. To enforce this, there should be universal standards and guidelines in place to guarantee that the VPNs are working as intended and protecting end-users from breaches.

Best Practices

Before installing VPNs, companies should choose the one that is best for its employees, but making that decision can be difficult due to the abundance of options available. There are a few things to consider before companies install VPNs and how to enforce best practices after devices are distributed to employees.

- **Free VPNs don't guarantee protection:** While free VPNs are present in the market, these options are not highly recommended since they typically collect users' data and sell it to third parties in exchange for there being no monetary cost. Even though free VPNs, and other mobile apps, are enticing, companies and employees are better off purchasing a VPN to ensure that personal and private corporate information remains secure.

- **Proactively check VPNs:** To make sure that a VPN is working, employees should check the location of the device. If the VPN is working properly, the device should display a location that differs from where the user truly is, remaining anonymous and undetected from hackers trying to find vulnerabilities.

A More Secure VPN Market

To create a more secure VPN market, there needs to be guidelines led by the industry to help keep companies and its employees safe. With these industry-led standards organizations, major technology, security and government stakeholders are working together to create scalable global standards and testing to ensure a higher level of security across VPNs that become certified through these programs. The security standards require VPNs to have security by default, standard cryptography, no universal passwords, automatic connection when in use, end-to-end encryption, and regularly released updates and maintenance. By implementing these requirements from the development phase, VPN services can assure companies and their employees that they will work as intended to protect them from bad actors and data exposure through their networks. This transparency will save companies time, money and headaches from rectifying issues in the long run.

As the remote workforce is here to stay, companies need to consider all security options before committing to one to protect data and sensitive information. When it comes to VPNs, organizations need to weigh the potential risks that come with these beneficial services in order to ensure all
devices and networks are properly protected. With global standards and guidance from industry organizations, companies can review and select a VPN that will best fit their needs, have better
insight into its security and flaws, and have greater confidence that it will work as intended - keeping all information safe from hackers.

About the Author

Brad Ree is chief technology officer of ioXt. In this role, he leads ioXt's security products supporting the ioXt Alliance. Brad holds over 25 patents and is the former security advisor chair for Zigbee. He has developed communication systems for AT&T, General Electric, and Arris. Before joining ioXt, Brad was vice president of IoT security at Verimatrix, where he led the development of blockchain solutions for ecosystem
operators. He is highly versed in many IoT protocols and their associated security models. https://www.ioxtalliance.org/

The Problem with Security Questionnaires

By Kelly White, CEO and Co-Founder, RiskRecon

Security questionnaires are one of the most prevalent and recognizable tools used to gauge and manage risks in third-party IT environments. Unfortunately, the popularity of questionnaires is more of a function of familiarity and expedience than a testament to their efficacy as a risk management tool.

When the rubber meets the road, most risk professionals admit they have very little confidence in security questionnaires. They don't think that these assessments provide an accurate view of risk exposure or give them an effective route for requesting remediation from third-party vendors. But running questionnaires is usually a straightforward, budget-friendly process. Vendors may not always like them, but they typically know what to expect from them. And more importantly, most regulators accept questionnaires as a means to checking many of the boxes for third-party risk management (TPRM).

And so, like firewalls and antivirus, they persist as a not-so-well-loved but de facto standard for their security domain.

According to the recent The State of Third-Party Risk Management Report compiled by Cyentia Institute on behalf of RiskRecon, as things stand today some 84% of enterprises employ security questionnaires. That's approximately twice the rate at which they use more advanced means of assessment like cybersecurity ratings to verify the security status of their third-party vendors.

The good news is that many organizations are innovating away from sole reliance on questionnaires. The study showed that 16% of vendors use a combination of security questionnaires, documentation review, remote assessments, cybersecurity ratings, and onsite assessments to round out their TPRM programs. Many others use a combination of two or three of those methods, with the most common backstop being documentation review, an assessment method used by 69% of organizations.

Nevertheless, a not insignificant ratio of TPRM programs—more than one in ten--still only assess via questionnaire. Additionally, digging into alternative assessment methods showed us that those are often only employed for a very small percentage of vendors. For example, while one in three TPRM programs incorporate onsite security evaluations, 60% of those do it for less than 10% of their vendors. So even when alternatives are employed, questionnaires are still the leading method for most assessments.

This is extremely problematic considering the results that TPRM professionals say they yield from these self-assessments. The survey showed that only about 34% of them say they believe questionnaire responses. That's likely because in spite of anecdotal industry evidence to the contrary and daily data breach headlines dominating the news cycles, some 81% of organizations report that the vast majority of their security questionnaires with no exceptions, claiming perfect compliance with requirements. Meaning that among those 81%,the net result is that their assessment rarely offered any kind of actionable insight to spur security improvements or remediations from vendors.

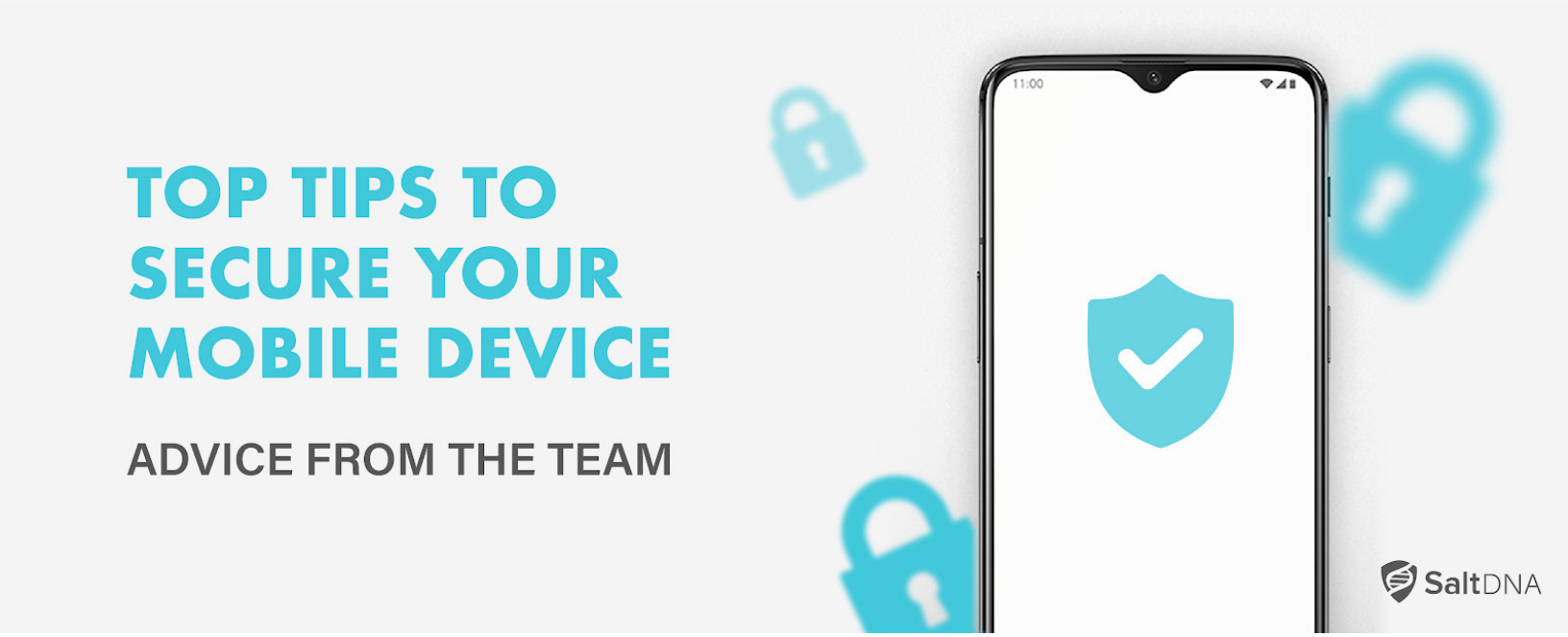
Clearly questionnaires are starting to feel like a rubber stamp, as very few TPRM professionals believe that vendor security performance truly meets their security standards outlined in the questionnaire. Only about 14% of organizations today say they're highly confident that vendors are performing security requirements.

Now, maybe part of that may be a function of how good of a questionnaire assessment most programs are putting in front of their vendors. Our study showed that under 20% of programs leverage an industry standard question set, and the majority of the questionnaires are usually under 100 questions in length. For about 11% of programs, in fact, the questionnaire is 10 questions or fewer. But the suspicion on the believability of answers remained consistent no matter how many questions were asked. So it seems that many organizations are starting to recognize that the only thing that can give them more confidence is to layer in more assessment methods and continue to deprecate the over reliance on questionnaires.

By moving to a data-driven third-party risk program, and by combining data from a wide range of sources--from a wide range of sources -security rating services, news feeds, financial ratings, and questionnaires—organizations can start taking their TPRM programs to higher level of maturity.

About the Author

Kelly White is the co-founder and CEO of RiskRecon, a company that enables dramatically better third-party security risk management outcomes. Prior to founding RiskRecon, Kelly held various enterprise security roles, including CISO and Director of Information Security for financial services companies. Kelly was also practice manager and senior security consultant for CyberTrust and Ernst & Young.



Top Tips to Secure your Mobile Device- Advice from the Team

By Nicole Allen, Marketing Executive, SaltDNA.

Smartphone users rely on their devices for just about everything: business, wallets, shopping, communication, entertainment- the list is endless. According to Statista, 3.8 billion people have a smartphone, and it is reported that the average user checks their phone up to 50 times a day. However, despite our reliance on our phones many do not use their devices safely.

Lapses in the most basic safety precautions could cause a whole organisation to be breached. To avoid having your organisations sensitive and confidential data from being attacked our team have put together a list of our top tips to secure your mobile device.

Encrypt hotspots from being used by other devices

Patrick Keehan- CTO & Co-Founder

Hotspots make your life simpler, giving you Wi-Fi, everywhere you go, at your fingertips. But if they are not secured, they can attack every device you have connected.

That's because hotspots will allow strangers without your knowledge to access data and files on your phone, tablet, and laptop. Protect against this by choosing a strong encryption for your hotspot, or the process of encoding a message. The default encryption may sometimes be outdated or not the most reliable.

Choose the most reliable hotspot encryption for hotspots, Wireless Safe Access 2, or WPA2, to prevent this. Originating in 2006, according to LifeWire, WPA2 has the best data encryption option. Although internet users may be able to see the traffic on a WPA2 network within range, the new encryption key will secure it.

Two Factor Authentication

John Bailie- Head of Marketing and Business Development

Extra steps may seem tedious but this isn't the case for two factor authentication. This will ensure that your identity is checked twice and is legitimate before gaining access into your device, besides passwords it will give you an additional layer of security.

A common type of two-factor authentication is one that produces a time-sensitive code that is sent via text message to your phone. The code is suitable for one-time use and you can access your account once you reach it. It's a little more work for you, but it makes compromising your account much harder for an attacker.

Updating your mobiles software regularly

Nicole Allen- Marketing Executive

You might find these updates coming up quite regularly but by keeping your mobile updated with the latest software updates it can reduce the chances of your phone being hacked. However, the longer you go without updating your phone and software the longer your data is at risk for any malware malfunction.

In reality, in popular applications, including operating systems and browsers, many of the more malicious malware attacks we see take advantage of software vulnerabilities. These are massive programmes that need periodic upgrades in order to stay secure and stable. So rather than procrastinating over software upgrades, see such updates as one of the most crucial steps to secure your information you may take.

Software upgrades may also provide new or upgraded functionality in addition to security improvements, or improved compatibility with various devices or applications. They can also enhance the software's reliability, and uninstall obsolete features.

Avoid charging your device in public ports

Sean Ashmore- Head of Android

This may hurt a little to find out, but charging your phone at public charging stations will make you vulnerable to a security breach, the kind found in airports, transit stations, airlines, conference and shopping centres. This is because your phone is more than charged by connecting to a public port, it also transmits data. If an outlet is hacked, then your emails, messages, images, and contacts may be accessed by a hacker.

According to Krebs on Security, a cybercrime and computer security news outlet, this technique of hacking phones is known as' juice jacking.' Your device is now infected by just plugging your phone into a (corrupted) power strip or charger and that compromises all your data.

Use a secure communications solution

Joe Boyle- CEO & Co-Founder

Having spent years speaking to businesses who have tolerated the unsecure exchange of confidential information we have seen a sudden realisation from these parties on the importance of using a secure communications solution. Not only does using a secure communications solution protect your business but it demonstrates a duty of care to clients and inspires confidence.

With the recent WhatsApp Privacy Policy changes the need for companies to use a highly secure, compliant and managed enterprise messaging platform such as SaltDNA, becomes even clearer. Facebook's exploitation of personal data means that many organisations find themselves at risk from a compliance perspective when conducting business over these consumer apps. It doesn't matter what type of company you operate in, your digital communications are probably regulated. These laws are not only in effect for your safety, but for the safety of your clients and customers.

At SaltDNA we work with organisations across the world of all sizes to enable them to have secure, confidential conversations wherever they are, at any time. Your best bet to ensure that the possibility of a cyber attack never becomes your reality is to enforce a secure communications platform alongside a comprehensive and ongoing employee education on cyber security.

With the increase in remote work due to COVID-19, the use of digital devices has now become an even larger part of daily life. There is an increased need to be more aware of cybersecurity and to secure mobile devices within your organisation. Users are capable of mitigating the possibility of cyber threats by introducing security measures. Following these top tips from the team enables employees to protect both themselves and the companies information, devices and overall privacy.

If you require further assistance feel free to reach out to our team for more information on this article. To sign up for a free trial of SaltDNA or to talk to a member of the SaltDNA team, please contact us on info@saltdna.com.

About SaltDNA

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

About the Author

Nicole Allen, Marketing Executive at SaltDNA. Nicole completed her university placement year with SaltDNA, as part of her degree studying Communication, Advertising and Marketing at University of Ulster. Nicole worked alongside her degree part time during her final year and recently started full time with the company having completed her placement year with SaltDNA in 2018/19.

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

Solarwinds Was A Dangerous Precedent – How Can the Supply Chain Be Secured?

By Gregory Cardiet, Senior Director, Security Engineering at Vectra

Supply chain cyber attacks are nothing new, but the latest SolarWinds incident is the starkest reminder yet that complacency comes with a price. The SolarWinds attack affected servers of at least 18,000 customers in the supply chain, many of which were high value government organisations.

Too many organisations remain overinvested in old-school perimeter defence solutions, such as sandboxing, IDS, and next generation Firewall, despite mounting evidence of their deficiencies, and simply 'building higher security walls' does not do the trick anymore. Furthermore, SOC still rely on very simplistic rules based on logs and looking for anomalies of user activities, making it difficult to find malicious offenders within the noise created by such rules. So, what can be done to fill the gap and prevent organisations from becoming a statistic in the next supply chain attack?

The common perception is that serious data breaches need to involve some kind of security flaw, for example, an application bug or vulnerability that attackers have discovered and exploited. The reality is that initial breaches are often the result of nothing more than very effective social engineering, and most supply chain attacks are no exception.

The first step of supply chain attacks will usually be to hit individuals at the organisation that produces the target software with phishing emails to harvest user credentials. Standard phishing tactics such as impersonating IT personnel or automated system emails are very effective here.

Once the attacker has compromised an account, they can begin moving laterally and gaining more privileged access until they can reach their target – the application's source code. From here, they will hide malicious code within the product, and then ensure that the company unknowingly pushes this Trojanised version out to it customers.

For this to be successful, the attacker needs their tampering to go unnoticed for as long as possible to give them maximum access to the product's userbase. To this end, the malicious code is likely inserted into the product just before it is shipped out, minimising the chances of it being detected through any security or quality assurance testing. In the SolarWinds case, the code was likely added to an update of its Orion software just before it was pushed out.

Launching a Trojan into the supply chain

Simply getting to the source code is not sufficient – the adversary needs to gain authorisation to publish as well. This means that, unless they are very lucky and find a privileged account with poor security, the attacker will likely be spending several weeks on very slow, careful lateral movement to reach their prize undetected. This will likely be a highly cautious approach that uses a "living off the land" strategy, exploiting native tools as much as possible to fly under the radar. The SolarWinds actors compromised the company's Microsoft Office 365 environment, including access to email and SharePoint among many other tools.

The adversary will also need to spend time researching the company and gaining a strong understanding of its operations before they even commence the attack. Once they have finally reached the source code, they will then need to be able to reverse engineer it to successfully add the malicious code without impacting the application's performance and leaving any obvious clues that something is amiss.

It's worth noting that this kind of attack requires a considerable amount of time and skill to execute successfully and has little direct return on investment for the adversary. As a result, supply chain attacks are almost exclusively the work of state sponsored threat actors. With a regular wage from their nation state paymasters, threat actors can comfortably spend several months planning and executing a supply chain attack even without a direct return on investment. The SolarWinds attack appears to have taken at least six months of work, for example.

When executed correctly, a supply chain attack is an extremely insidious technique that is extremely hard to detect. SolarWinds was only eventually discovered because FireEye suspected something unusual was happening and took the time to investigate. It's very likely that many other software companies are under the influence of similar attacks but have not yet discovered them.

How supply chain attackers hide in plain sight

The most devious thing about a supply chain attack is the way it hijacks legitimate software delivery to reach a huge number of victims. Sunburst, the malware that infected SolarWinds' Orion software, is believed to have infected the servers of at least 18,000 customers.

Once the Trojanised software has been installed by the customers, the threat actor can execute the malicious code to continue the next leg of the attack. In the case of SolarWinds, the main objective appears to be reconnaissance, and it is speculated that the perpetrators used it to gain a critical understanding of the operations and tools used by the customer companies – in this case primarily US governmental agencies. While quiet observation was the goal here, supply chain attacks like this could also conceivably be used to launch large scale, debilitating cyber attacks striking multiple high value targets simultaneously.

Another significant factor in the attack is the extraordinary dwell time the adversaries achieved. It was eventually determined that Orion updates between March and June 2020 had been infected with Sunburst, with the breach not being reported publicly until December 2020. This indicates a timescale of several months where attackers had free reign in the SolarWinds supply chain, and an even longer period within SolarWinds' own systems.

Investigations have noted several tricks used by the attackers to mask their presence of such an extended period. Commercial cloud servers such as Amazon, Microsoft and GoDaddy were used to host the command-and-control centres for the attack, making it much easier to hide communications in mundane traffic. Much of the malware used in the attacks were also newly created, and therefore did not match any known threat signatures.

Traditional detection tools won't cut it

The biggest takeaway for any organisation from the SolarWinds attack is that they can no longer rely on traditional signature-based threat detection to keep up with malicious activity. The SolarWinds attack was so successful in part because the adversaries left almost no traditional indicators of compromise. The organisations infected by the Trojanised Orion software were entirely blind to the intruders in their networks.
The use of legitimate cloud hosts for the C2 traffic also meant communications were well hidden from standard detection tools, and this is an approach we are seeing more of in the wild. Even resources like Dropbox, Twitter and Slack have been subverted into C2 channels.

Similarly, attackers "living off the land" using legitimate capabilities from Microsoft Office 365, including email, SharePoint, and others such as Power Automate and eDiscovery, are able to hide in plain sight for extended periods of time.

Detecting this kind of careful and sophisticated attack means going deeper and looking for subtle signs of suspicious activity that may indicate a compromised account attempting to achieve lateral movement. One of the most effective weapons to fight against this threat are Network Detection and Response (NDR) tools powered by AI analytics. These solutions continually monitor the entire environment, spanning both traditional IT and cloud networks, to rapidly detect signs of compromise.

The power of AI analytics means huge amounts of data can be crunched in moments, accomplishing in a couple of hours what would otherwise take days of intensive work from human security analysts.

This capability means that, even if threat actors infiltrate the network with a technique as devious and subtle as a supply chain attack, the security team have a strong chance at identifying and stopping the attack before it can escalate. Likewise, the software developer being targeted to propagate a supply chain attack will also have a much better shot at detecting intruders creeping their way through the network towards their source code. The ability to spot and halt a sophisticated and careful attacker before they can Trojanise the product will stop a single breach from spiralling into a major incident that impacts thousands of customers in the supply chain.

About the Author

Gregory Cardiet is Senior Director, Security Engineering at Vectra. Gregory has been working in the field of cyber-security for the last 10 years, first focused on Networking and now Cloud security. During the last 4 years at Vectra, he has been evangelizing the idea of a need for a next-generation of network-based detection and response tool (NDR) that would close a gap created by EDR and SIEM. Previously, he has held a role as Consulting Security Engineer (Expert) at HPE/Aruba where he was advising large global organization about security strategy of the access layer.
Gregory can be reached online at linkedin.com/in/gcardiet and at our company website https://www.vectra.ai/

Stopping Threats Requires Early Detection of Attacker Lateral Movement

By Jeff Barker, VP of Product Marketing at Illusive

As the recent rise in successful ransomware attacks shows, cybercriminals have shifted their focus from consumers to highly targeted attacks on enterprises, leveraging tactics and techniques taken from the Advanced Persistent Threat (APT) playbook. But if you think APTs are yesterday's news, look no further than the 2020 cyberattack against SolarWinds to show how risky and exposed to hackers improperly secured networks and systems can be.

Although this kind of supply-chain breach relies on techniques and vulnerabilities that are common, the SolarWinds incident is only the latest evidence that supply-chain breaches are extremely difficult to stop. These highly sophisticated attacks focus on obtaining credentials, followed by a low and slow lateral movement approach to reach crown jewel assets with the aim of gaining untrammeled access to systems and data—a catastrophic business outcome if not discovered and stopped in time.

The sheer size and scale of the SolarWinds attack indicates that traditional attack mitigation strategies and technologies are not adequate on their own for stopping human-guided attacks like APTs or advanced ransomware. If an organization isn't using technology that can detect and stop the lateral movement component of a typical contemporary cyber-attack, they will continue to be vulnerable and at-risk of a successful incursion. Organizations must augment their strategies to stop human-operated attacks as they move through their networks and prevent them from accessing systems and endpoints at scale.

Why are lateral movement attacks still happening?

With great opportunity comes great evolution, and the lateral movement attacks of the 2020s are more sophisticated than ever before. These kinds of attacks are now so prevalent that they're used in nearly every other kind of cyber-attack, even though the time it takes to detect a network intrusion dropped from 418 days in 2011 to 78 days in 2019. Once an attacker is able to establish a beachhead, they can cause massive amounts of damage to organizations and even force them out of business.

There are several reasons why lateral movement attacks are still happening: 1) the size of the attack surface makes it difficult to prevent attackers from establishing a beachhead; 2) the attacker has access to increasingly sophisticated tools; and 3) limitations in our existing security controls for detecting and preventing lateral movement.

A notable recent contributor to the increased attack surface is the current pandemic forcing employees to work from home (WFH), expanding the attack surface far beyond what security teams expected to manage. Employee home networks rarely have the security controls in place that corporate networks do, from security appliances to management software. The WFH user can represent an easier target for threat actors to establish a beachhead, and once compromised, can offer a path to targeted crown jewels. Moreover, the shift to work from home significantly changed the behavior defined as normal by anomaly-based detection systems, resulting in a significant increase in false positive alerts. It's difficult to establish a baseline for behavior-based detection when nearly everyone's behavior patterns are changing.

To better exploit this extensive and changing attack surface, attackers have easy access to increasingly sophisticated tools. For example, they can access easy to use Ransom-as-a-Service (RaaS), with a sophisticated toolset, in exchange for splitting their payouts with the RaaS operator.

Current security controls are more focused on the perimeter, defensive in nature and relying on signatures and anomalies for detection. When the attacker circumvents the perimeter, it's far too easy for them to move laterally without detection. Threat actors look to move laterally within networks because before they can steal data, they need to understand what data is available on the network in the first place. While extended dwell time makes it easier in some cases to detect and stop the threat actors before attacks can hit paydirt, it also means that a straightforward endpoint threat detection and response (EDR) will not always detect activity leveraging legitimate connectivity and normal behavior to avoid anomaly-based detection.

EDR is an important endpoint security control to monitor and protect endpoints, but this technology is challenged to identify when the attacker is not behaving differently than the user of the breached system – and is moving laterally leveraging authentic credentials and normal connections and pathways. Furthermore, EDR is increasingly targeted by attacker techniques to disable and circumvent as part of their beachhead establishment and persistence tactics.

How to change from reactive defense to active defense

MITRE, the 62-year-old nonprofit dedicated to creating engineering and technical guidance for the U.S. government, recently created an active defense-focused knowledge base it calls Shield.
MITRE Shield is a set of best-practice recommendations for organizations from practitioners to executives. Shield includes structured elements such as data tables connected by links, as well as less structured - but no less important - concepts and explanations, such as those found in blog posts. It includes recommendations for basic cybersecurity hygiene, as well as advanced defensive techniques covering deception and adversary engagement.

The goal, wrote MITRE in its introductory blog post about Shield, is to allow "an organization to not only counter current attacks but also to learn more about that adversary and better prepare for new attacks in the future." At its core, active defense seeks to create a hostile environment for the attacker, raising the cost of hacking to a level where it becomes unattractive to the threat actor.

Raising the cost of lateral attack movement with an environment hostile to attackers creates a situation where even sophisticated adversaries are unable to move laterally without detection. With a deterministic detection approach, it's possible for an organization to gather valuable real time telemetry to understand their target, remediate and adjust security strategy and tactics to safeguard against similar attacks in the future.

The SolarWinds attack indicates that there are shortcomings in existing security controls to ensure adequate credential and connection hygiene and prevent undetected lateral movement.

Organizations need to adopt an active defense strategy to make it more difficult for attackers that have established a beachhead to move laterally without detection and achieve their objectives.

About the Author

For more than 25 years, Jeff has been leading teams to pioneer disruptive network, data, and security solutions to improve the performance and security of infrastructure and organizations. Now as VP of Product Marketing for Illusive, Jeff is focused on helping organizations understand how adopting an offensive security strategy with Active Defense can change the game on the attackers, giving the defenders a long overdue advantage

Learn more about him at https://illusive.com/

The Cybersecurity Risk Posed by Your Outdated ETRM System

Is your ETRM system leaving you exposed to hackers?

By Kent Landrum, Managing Director, Opportune LLP

Energy or commodity trading and risk management (ETRM or CTRM) systems have been gaining momentum since the 1990s and continue to be at the heart of many energy companies' information technology landscapes. In many cases, these applications have been developed and continually enhanced over a period of decades and carry with them a legacy of outdated technologies and software development standards. While major ETRM vendors have made improvements to their platforms in recent years to address these limitations, relatively few customers stay on the leading edge of software releases. In addition, most of the traditional ETRM solutions were originally developed as on-premises solutions and most clients continue to operate them this way. These, and other factors, combine to create the potential for a significant cybersecurity risk.

Many companies made significant investments in terms of time and money in the original implementation of their ETRM solution. Over the years, however, these applications have become increasingly integrated with other key enterprise systems like enterprise resource planning (ERP), data warehouses, as well as to external parties such as exchanges/brokers and market data services further expanding cyber risk profile. The initial capital outlay and recurring operating expense has left little appetite for additional patching or upgrades in the absence of a key new piece of functionality demanded by the business to drive a benefits case in spite of the fact that it's exactly these steps that serve to reduce the potential exposure.

The Cyber Risk

Energy companies are known to be top targets for malicious actors—particularly those of the state-sponsored and "hacktivist" varieties. Outdated software at any level or layer of the ETRM solution architecture presents a security vulnerability that these cyber threat actors will seek to exploit. Oftentimes, older applications are incompatible with the latest, most secure operating system (OS), database (DB), and runtime software so these key components also can't be upgraded. A greater number of older components increase the potential attack surface, and the more aged they are means there are more known exploits available to any would-be hacker.

This software patching "log jam" created by an out-of-date application results in situations like:

- Running older versions of Java, the .NET framework, etc.
- Using past versions of an SQL server or Oracle databases.
- Hosting the application and database on obsolete versions of Windows or Linux.

In more extreme cases, this situation can spiral out to middleware software, custom integration, and touchpoints with third parties such as price data and measurement services. Custom code can be at an increased risk for exploits like credential stuffing or SQL injection, among others. Taken together, these gaps can leave your IT systems exposed to dozens, if not hundreds, of potential cyber exploits. It's not just about malicious actors gaining access to sensitive trading data, or that they could take a critical commercial and risk system offline, but that the ETRM can be used as a platform to attack other assets on the business network.

Mitigating Actions

The obvious answer is to upgrade the ETRM system, but it can be challenging and time-consuming to build a benefits case, gain approval, and secure funding for a large project. While an organization considers the longer-term prospects of an upgrade or potential re-platforming initiative, below are steps that can be taken immediately to reduce the risk of a cyber incident.

- Apply the latest versions and patches of the OS and DB that are compatible with the ETRM vendor's software—same for components and frameworks like Java and .NET.
- Harden your DB and application servers by removing unnecessary components and access, closing ports, limiting RDP/SSH to whitelisted IP addresses only, etc.
- Run vulnerability scans on your ETRM system's servers and remediate identified issues by priority.
- Use secure connections running current cryptographic protocols such as TLS (Transport Layer Security)—note that SSL has been deprecated due to known vulnerabilities.
- Consider enabling data encryption in-transit and at rest (either in the DB or storage layer) where feasible.
- Conduct static and/or dynamic code analysis on all custom interfaces and components and remediate security defects by severity.
- Ensure that end-point protection is in place for all devices from the end-user's system, through remote access like Terminal Server or Citrix, to the middle tier and database servers of the ETRM itself.
- Enable logging and leverage a SIEM (Security Information and Event Management) solution to detect unusual activity and provide early warning of a potential breach.
- Segment the network to put legacy systems in their own "box" where access to/from can be limited to those individuals and systems that truly have a need.

The items listed above cover a wide range of cost and complexity, can be implemented in a variety of logical sequences, and can be paced in a manner that's achievable by most IT departments.

Conclusion

At a time when IT, risk, and commercial leaders are being asked to do more with less it can be difficult to justify large investments like those necessary to upgrade or replace an ETRM system.
However, the very real risk posed by a potential cybersecurity breach demands prompt and prudent action to be taken to secure the systems comprising a company's trading and risk IT
landscape. Actions like those previously recommended can go a long way in reducing the ETRM system's potential attack surface and become a harder target for cyber threat actors.

About the Author

Kent Landrum, Managing Director in Opportune LLP's Process & Technology practice who leads the firm's Downstream Sector, has 20 years of diversified information technology experience with an emphasis on solution delivery for the energy industry. Kent has a proven track record of managing full life cycle software implementation projects for downstream and utilities companies, including ERP, ETRM, BI, MDM, and CRM. Prior to rejoining Opportune, he served as a Vice President & Chief Information Officer for CPS Energy. Kent holds a B.S. degree in Computer Science and Economics from Trinity University and a master's degree in Organizational Development from the University of the Incarnate Word.
Kent Landrum can be reached by email at klandrum@opportune.com, Kent Landrum | LinkedIn, Twitter @KentLandrum1) and at our company website www.opportune.com

The Truth About the Real Impact of SMB Website Breaches

By Ed Giaquinto, CIO at Sectigo

You've set up your website, you've brushed up your digital strategy, and you're finally ready to shift your focus to other priorities—but did you remember to lock up?

If you're like many small-to-medium-sized businesses (SMB) website security decision-makers, you may think your business is too small for hackers to take notice or that a breach won't happen to you. But you can't just call up cybercriminals and ask them not to hack your site or force an outage. So how are SMBs faring if most are overconfident and not equipped to combat cyber attacks? We recently conducted a global survey of 1,100 SMBs to understand better the role websites play in each business, the degree of risk these sites represent, and how prepared SMBs are to secure them. Let's take a look at what the data says about the impact of website breaches. Disclaimer: this is not for the faint of heart!

Half of SMBs Have Experienced a Website Breach

There's no sugar-coating it. 50 percent of SMBs experienced a website breach, and 20% of our sample experienced one just in the past 12 months. And these are the ones who even know they were breached! The actual numbers are likely significantly higher. If you're in FinServ, things look even more dire, with 52% of SMBs with reported breaches in the past year. Worse yet, in China, 66% of SMBs say that their website was breached in the past year. I think we can all agree that website breaches are far too common.

The Impact of Website Breaches Is Severe

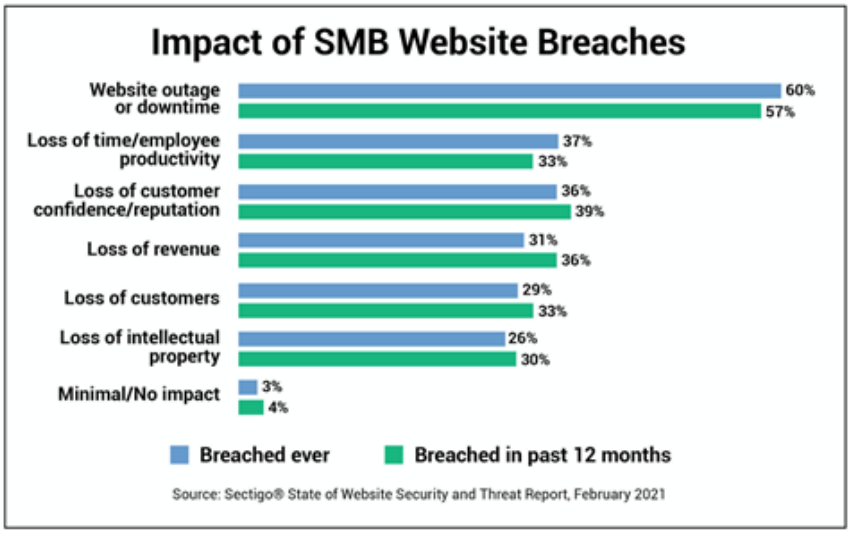
Websites today are the face of the business to most customers and increasingly drives a significant portion of revenue. 54 percent of SMBs say there would be a serious impact on their business if their website went down, and 72% say they collect or store sensitive data through their website. Not long ago, a breach that compromises personal information like credit card information and social security numbers would have made headlines.

Only 3% of businesses who were breached said there was no impact, and the number of businesses where breaches led to **revenue loss was about ten times that**

Now, it's so common we don't always hear about it happening. The impact of these breaches, regardless of whether they constitute a top news story, is severe. 28 percent of those who had been breached said the consequences were severe or very severe. The top three impacts were website outages or downtime, loss of time/employee productivity, and loss of customer confidence/reputation. And as most business owners know, any of these impacts can lead to lost opportunities for more sales.

#1 Impact: Website Outages or Downtime

Your website is often your business' first impression, how you connect with your customers, and how you make sales or give information - 24/7/365, even when you're asleep. But your online business is entirely unavailable during a website outage, and customers land on dead pages or are even redirected to malicious content. In most cases, if your website is down, your online business comes to a screeching halt. Leads stop coming in, there are no transactions, and ads are wasted. In the era of COVID, when the means of doing business hinges on a seamless online experience–outages aren't an option. Of SMB websites that were breached, 60% of attacks resulted in site outages.



#2 Impact: Loss of Time/Employee Productivity
A breach is felt deeply within an organization. The business disruption that follows is damaging even after disaster recovery and business continuity efforts. When business leaders and employees are sorting through issues such as customer complaints or legal inquiries, scrambling for makeshift solutions, and sorting through the aftermath of an attack, productivity goes down the drain, and day-to-day business operations suffer. Of SMB businesses whose websites were breached, more than a third incurred time and employee productivity losses.

#3 Impact: Loss of Customer Confidence/Reputation
The long-term effect of your business' damaged reputation may be a much harder pill to swallow than short-term losses. Of SMB websites that were breached, 39% of attacks resulted in customer confidence/reputation loss. If your organization is seen as vulnerable, such as if your customers' information is compromised or simply if your website cannot be accessed, customers and potential customers may look elsewhere to do business. And they are likely to never come back. Business owners are all too familiar with fierce competition and are wise to raise this point to their organization's website security decision-makers.

There's No Margin for Error
When it comes to website security, SMBs are vulnerable. There's a high cost to believing that a breach won't happen to you. Consequences are devastating, and the impacts range from short-term losses to permanent damage. There's also a clear advantage held by organizations that have invested in a holistic, end-to-end approach in a single solution. In an age where there is no margin for error in gaining and keeping your customers' trust, it's time to invest in solutions and partnerships that will grow and evolve as threats and attack vectors evolve.

Download the full Sectigo State of Website Security and Threat Report to learn more about the constant attacks that SMBs face and the website security solutions to deal with them.

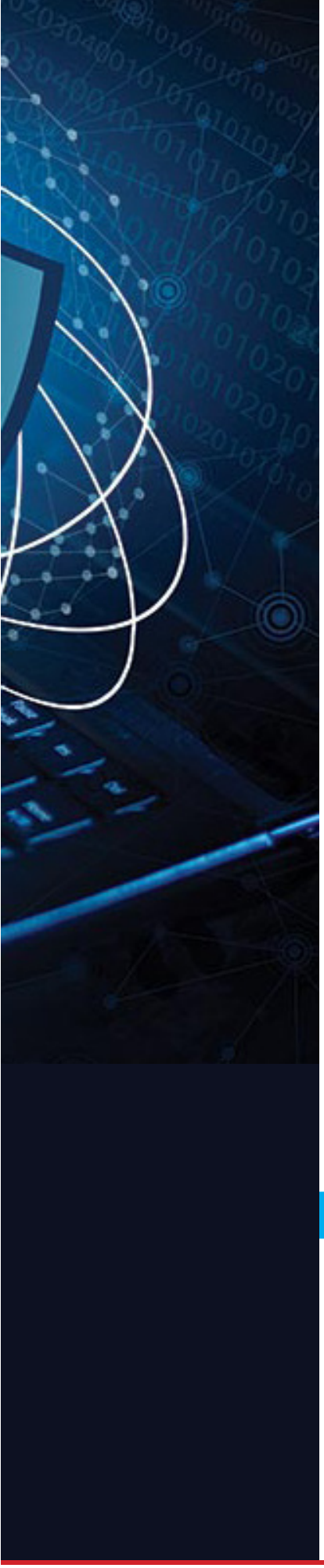
About the Author

Ed Giaquinto is CIO at Sectigo, a global provider of digital identity management and web security solutions. As CIO, Ed Giaquinto oversees IT and support, leading initiatives around change control, onboarding, proof of concept (POC), customer communications, service, and innovation in operational practices. Ed assumed the role in February 2019 following his role as Sectigo's VP of Information Technology, where he led strategic planning and IT process development gleaned from 30 years in the IT industry.

Ed can be reached online at https://sectigo.com/ and at our company website https://sectigo.com/

Tips to Combat New-Age Digital Security Attacks for Enterprises

By Harjott Atrii, Executive Vice-President and Global Head, Digital Foundation Services, Zensar



Digital organizations are here to stay, as increasingly it is imperative to have digitization, driven by cloud first mindset, at the core of every business operation. The vision of a digital enterprise cannot be realized without securing each byte of data inside every database or billions of IOT devices that sprawl the connected world, which is rapidly adopting hybrid-cloud and multi-cloud as the inevitable foundation of IT. The recent pandemic has led to an acceleration of this need to digitize and automate business processes. We are experiencing a radical transition in enterprise behavior that aims to thrive in a distributed ecosystem by designing any application and any database in a compute neutral and cloud neutral fashion. However, this has led to a considerable increase in the risk of cyber-attacks. Moving to the secular cloud, implementing new technologies like connected edge cloud, etc. has led to almost an end to secure networks and central monitoring of security risks. Currently, most of the larger global firms are encouraging their teams to continue working from home remotely. This factor adds to the overall risk posture. As organizations become readily dependent upon internet-enabled business models, they are more vulnerable and prone to a wide array of cyber-attacks and business disrupting challenges.

We have recently witnessed a huge security threat when the malware called Emotet broke out across. It has been termed as one of the most dangerous malwares, ransomware attacks in recent times. The effort taken to control it involved various government agencies working together to bring it under control. According to experts, in 2221 and beyond cybercriminals will unleash the fifth-generation cyber-attacks, while 97% of the world can protect itself only from second and third-generation attacks. And reports suggest that cybercrime may now cost the world almost $600 billion, or 0.8% of global GDP. These sophisticated attacks might give a negative impact on the digital economy and make them more unstable on each successful attack.

Cybercriminals are now more sophisticated and targeted; hence it is now critical to adapt to the best security strategies and practices to reduce the impact on business
.

Here are some tips for enterprises to combat the cyber-attacks: -

1. Choose Agile IT and redesign to adopt a secular cloud

Agile IT means bringing agility to your IT infrastructure and operations by transforming infrastructure across edge, core or public cloud and security from a reactive, 'ticket driven' approach to a proactive approach incorporating predictive threat-hunting, threat intelligence, security for APIs, etc. Build a secular multi-cloud operating model that combines cloud-based digital technologies and agile operational capabilities in an integrated and sequential manner. Build a cloud-native security model enhanced with DevOps.

2. Keep a Hawkeye on your relational and unstructured data and ensure its protection

Organizations must conduct a periodic audit of all data, including databases, data warehouse, data lake, data marts and other sources to identify where the sensitive data resides and remains overexposed. It is important to have details on who has access to the data and under what circumstances, who is the authorized owner and where it is required to revoke the access from the data. These things can be achieved by using the specially designed solution, data governance, and classification after consulting the data security experts according to the requirement. It helps organizations to have more granular control on all their data types- no matter where it resides, whether in the cloud, SaaS, or traditional data centers. Based on the criticality of data, one should implement the security policies and safeguards. There is a need to implement higher security controls with D-A-R, D-I-M encryption and have the least access rights to data that will impact your business greatly if lost or stolen. Follow the compliance guidelines based on data types and geographies. Develop a privacy policy and adhere to it strictly. While all these stringent data security measures need to be deployed at scale, it is extremely important to keep consumer grade experience, enterprise grade governance with integrated multi-cloud data and database management at the forefront of all design methodologies.

3. Adaptive Multi-layered defense approach

While it takes a long time to build a reputation, it can get compromised in a matter of few minutes due to an occurrence of a cyber incident. Thus, preventive and proactive defense posture is much needed.

Highly sophisticated and targeted attacks are very hard to detect and like with any criminal activity, it's not possible to detect 100% of the threats all the time, but there are always ways to mitigate those threats and reduce the impact. Traditional security methods like AV, FW, IDS/IPS are no longer effective on their own because of mobility, cloud and now many organizations have borderless entities that enable users to access corporate resources any time and from anywhere. Adaptive multi-cloud data and security models can help organizations by automatically analyzing the behavior of threat activity, finding anomalies, and creating a sequential and detailed analysis of threat events for better visibility, detection and prevention that combines to become more effective. Integrating with other security tools, implement layered defense approaches like paired with layers of enterprise endpoint security tools, EDR/XDR, data security and monitoring, adaptive security can help enterprises to prevent an attack from occurring and respond to breach in a timely fashion, that minimizes the impact and saves the reputation.

4. Innovative and Offensive Strategy with multi-cloud at its core

In this fight to prevent a cyber-attack, often cybercriminals are sometimes ahead because they are willing to innovate and continuously try to infiltrate the organization to gain access to corporate resources and confidential data with their highly sophisticated and innovative TTP (tactics, techniques and procedures). Businesses and enterprises need to do the same to save themselves from cybercriminals. So, they should architect IT to thrive in a secular multi-cloud ecosystem through normalized experience for all data sources including heavy-duty large databases and invest in innovative solutions, address the latest security issues, keep themselves updated, have a strong lifecycle patch management and efficient cyber workforce to innovate and hunt the latest threats before they hit the environment. Enterprises must invest & focus on innovations and proactively hunt for evolving attacks, and threat vectors and resolve the skill gaps of the cybersecurity workforce gearing up with block-chain based data protection, adaptive IDAM, and automated data rights revocation.

5. User Awareness and Accountability

The only way a cybersecurity strategy can be a success, is when organizations keep the focus on basic security hygiene. It does not matter how well you configure your security controls; this will be moot until you have trained the users on how to use them. A single click on a malicious URL can give control to the attacker to open the backdoor and penetrate corporate defense.

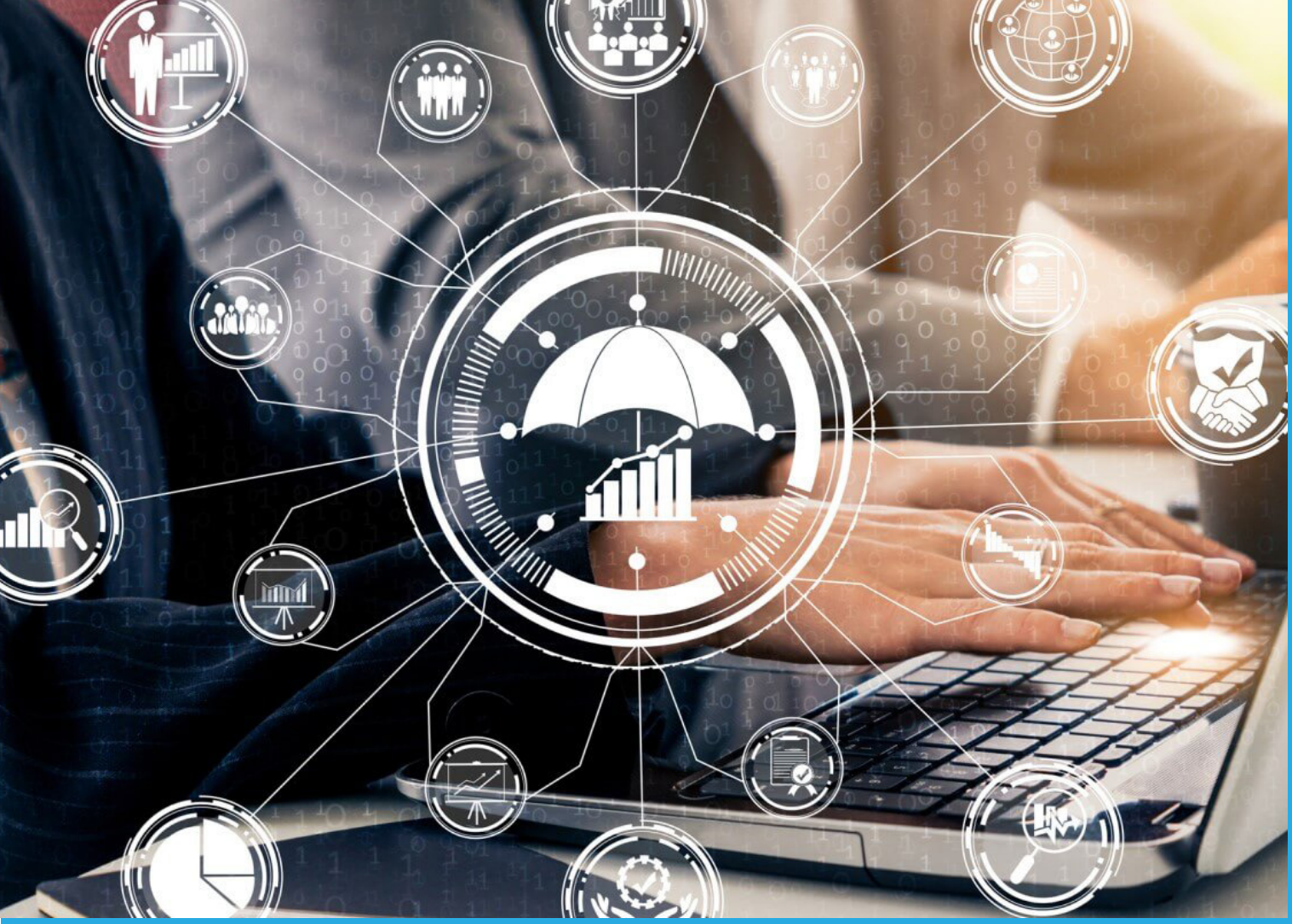
Security is as strong as the weakest link and humans are that weakest link in the system making a favorable target for cybercriminals. To keep secure, organizations must implement cybersecurity policies and train the users on how to use and make user accountable and responsible for corporate security. Formal security training, mandatory InfoSec training, timely educating users via mailers, security advisories, webinars, etc. helps to protect users and your enterprise from cyber-attacks.

While, there is no foolproof way of warding off cyberattacks, with the proliferation of everything digital bolstered by the adoption of the secular enterprise multi-cloud ecosystem , the first step begins with proactively recognizing the need. Additionally, there needs to be a strategic approach, and not a piecemeal one. The above tips should help in building a strong cyberattack defense eco-system that protects any data and database on any compute and fosters the notion of normalized experience across the multi-cloud ecosystem.

About the Author

Harjott Atrii, Executive Vice-President and Global Head, Digital Foundation Services, Zensar. He has twenty three years of experience in IT services industry, with successful track record of selling complex application outsourcing (AO) and infrastructure management outsourcing services across industry segments viz. Financial Services & Telecom; generating high value sales in USA, UK, Ireland and Middle East region.

Harjott can be reached online at https://www.linkedin.com/in/harjottatrii/ and at our company website zensar.com



Understanding the Risk of Supplier Management: A Six-Pronged Approach

By Aaron Kiemele, Chief Information Security Officer at Jamf

Years ago, I heard a story where thieves broke into a datacenter through the roof and lowered themselves, ninja-style, on cables. Seriously. Ninjas. On cables. Though rare, attacks such as this do, in fact, happen.

But far, far more likely? A nondescript person approaching the locked door, their arms full of boxes, asking for someone to let them into the office. Someone finding a dropped key and pocketing it. Someone figuring out that the side exit door never quite clicks shut unless someone leans hard on it.

This applies to cyberattacks as well. Some will be planned as a full-frontal assault from a nation-state type actor. But most? They'll sneak in through your weakest access point.

In the past, security professionals went by the old 'protecting us from ninjas' model. It was all about your perimeter. You had a firewall, a data center, all your secrets were locked behind concrete. It was all about guarding the doors and windows (and, perhaps, as in the previous rare case, the ceiling).

Much like a stealthy ninja, even the best and most robust security systems can neither detect nor protect against a fail on someone else's system or falls outside of the scope of the security system's capabilities. Consequently, the most common way to think about security is: where is your risk? How can you mitigate it?

Increasingly that risk is supplier management, exposing your business to the risk of a software vendor's vulnerability.

Extent of the problem

Who outside of security professionals remember the details of how a company was breached? When it hits the news, everyone knows who got breached, but not much else. All breaches sound bad in a newspaper or blog post: they lose their customers' data and they lose their customers' trust. Did it really matter that the issue started with a third-party problem in a periphery device in a retail store or a vulnerability in a product without obvious direct access to data? It makes no difference. Their security failed. That is what people remember.

Often it failed because of a third-party integration, but that nuanced story is pointless. Not that they didn't make their own set of mistakes, but in most cases where there's a breach— even when it's terrible — security teams tried their best to do the right thing, and they fell to something on the margins.

And third-party breaches continue to dominate the headlines.

For instance, the SolarWinds breach [link: https://www.cnet.com/news/solarwinds-hack-officially-blamed-on-russia-what-you-need-to-know/] almost certainly will go down as one of the biggest, most serious breaches in history.

The breach here wasn't a "hack" like in the movies; instead it was a seemingly valid patch to a great tool IT teams are using every day.

Their customers were now exposed through no fault of their own and now the companies themselves have to deal with the potential fallout and probable future attacks stemming from this leak.

The ultimate consequences of this vulnerability are still opaque, but at the very least attackers got privileged access into many global companies and government entities.

While there are innumerable causes for a security failure, the public sees it this way: if you fail, you fail. So how do you cover for this risk, and how do you reduce risk in the supply chain?

Turns out, that can be really tricky if you depend on only one way of doing things. You've got to have a multi-pronged approach.

ONE: Vendor Screening

This type of risk has hardly been invisible. Many organizations have a Security Assurance Group: staff members who focus on answering supplier management questions for customers, to assure them the risk is manageable. Many companies require prescreening and for vendors to follow specific security protocols.

Although this step can eliminate working with truly unsafe vendors, due diligence can go something like this:

Q: Do you make terrible security mistakes?
A: We do not.
Q: Do you lock your doors?
A: We do.

There are varying degrees of vigor, but by and large, they're pretty straightforward. They can be an effective way of performing due diligence, but in the end, does vendor screening by itself get you to increased security? Can you be assured of your safety?

There is no single-threaded solution to risk; you need to do more.

Keep in mind that there is no perimeter anymore; we are all zero trust now whether we are prepared or not. It's important to note that risk cannot be eliminated. It's inherent in doing business and can only be mitigated. The question is this: what steps can organizations take to minimize risk from their third-party vendor pipeline? It's safe to assume that, even after doing your due diligence and vetting your supply chain, someone is going to be compromised. Assuming this to be true and covering all of your bases fully expecting such a compromise will put you in the best position.

TWO: Balance of security and vulnerability

It's simply impossible to do business now without using multiple vendors expanding your risk profile dramatically. Everyone is doing their best to mitigate security issues with due diligence and supplier management processes, but the problem is that there are a million applications. All of them could have some sort of security issue and many could be in use in your environment.

Security is a business enablement function but my instinct is not immediately to support productivity as a singular goal.It's to reduce risk by finding a balance between productivity and risk. Know what your business needs to maximize its productivity and effectiveness, but also understand your tolerance for risk. What can the business accept and what can it not? This can form the basis for making informed decisions about supplier risk.

THREE: Real risk mitigation is in the basics

Nobody is excited about this problem. There is absolutely no one announcing with pride their Computer Science major in Supplier Security Management.

So many people go into security thinking: "I'm gonna hack the planet and pen test everything," —and there is real value there— but often the best security is found in more mundane activities. Do I know what is in my vendors' change logs? How quickly can I evaluate and patch 100 applications . . . or a 1,000?

These are not exciting questions; they don't have an inherent sense of drama. But they are critical questions.

So what do you do, assuming that of your hundreds of vendors, at least some will have a breach in the next year?

You focus on the fundamentals:

- asset management
- identity and access management
- vendor due diligence and annual review
- robust and timely maintenance
- vigilance

FOUR: You've got to see the problem

A central issue is visibility. How do we determine that an application has a patch available for a serious issue? There isn't necessarily a foolproof way to determine that at scale, but you have to do your best.

Most companies use the Common Vulnerability and Exposures (CVE) [link: https://cve.mitre.org/index.html] mechanism; this is a giant database governed by the public and private sector volunteers that lists all the vulnerabilities on most products.

But this depends on the company to be forthright about it. It's totally voluntary.

And companies can choose how to word the notices — some companies might be more interested in downplaying the issue than clearly explaining the problem, but in large part the data is good.

Though not comprehensive, it's one of the best tools we have, and regular scans of CVEs as well as regular reviews for patches in third party software will give you visibility into what existing, known problems you need to address.

Asset management is a security fundamental, you need to have a good sense of what happens on devices especially those where an employee has wide discretion to install applications without top down Security or IT involvement.

Chief among these are:

- what software is installed
- what services you use
- what you connect to (OneDrive, SharePoint, Dropbox, etc.)
- what does a "normal" system look like and how does it behave

Although this might not tell you exactly which vendor has a vulnerability, it will help you to keep an eye on entry points that are possible, and you can tighten up those entry points as much as possible by allowing only certain types of software, ensuring that where services interface with your own stack you've put some safeguards into place, and locking down those permissions as tightly as you can.

You need visibility into these questions: logs that are useful and sortable, an accurate inventory, and an awareness of the places you connect to others in your security framework.

And you need to have a strong focus not on an impenetrable security system (as we've shown, there is no longer any such thing), but on mitigating, rather than eliminating, risk. All you can do is drag the risk into the window that you can tolerate.

A good device management system with a strong inventory and permissions feature can help Security and IT sort through what happens in the event of a compromise of their internal systems after the fact, and push out a fix as quickly as possible.

FIVE: Stick with Security 101

You do all the things you learn about in Security 101. You do them well. You do them consistently. You review, and you do them again.

Can you answer these questions to your satisfaction?

- Have you reviewed and ensured strong configuration management for your devices? You'll need a good MDM to stay on top of that.
- Can you effectively say who has access to what?
- What is your identity and access management solution, and what are its security vulnerabilities? State of your system
- Do you know everything that is running in your environment?
- Do you know what their patch status is?
- Do you know how many published vulnerabilities there are?
- Do you know what state individual workstations are in?
- Can you track this? Can you verify that it's correct?

SIX: Consistent tracking and remediation, or: finding weird stuff

Effective endpoint security, effective monitoring and visibility and an effective system to set a response to patches can set you well on your way. Effective patching on a well-understood cadence based on this tracking is crucial.

If something weird happens, like 1500 logins for a user in a country you don't do business in, or from one dude in marketing (which is totally a true story), will you see it? Does your setup notice that sort of thing, and does it highlight things that are strange quickly?

Behavioral security doesn't just guard against known malware. It looks closely at activity, and at what is unusual or suspicious activity. What's weird, in whatever scenario? JavaScript running or programs downloading payloads in the middle of the night? Good behavioral endpoint protection identifies activity that acts like a virus or like a setup for malware, sandboxes it and reports it. In our current security climate, you can't really afford to not understand and measure for anomalous behavior.

Mitigation, not lockdown

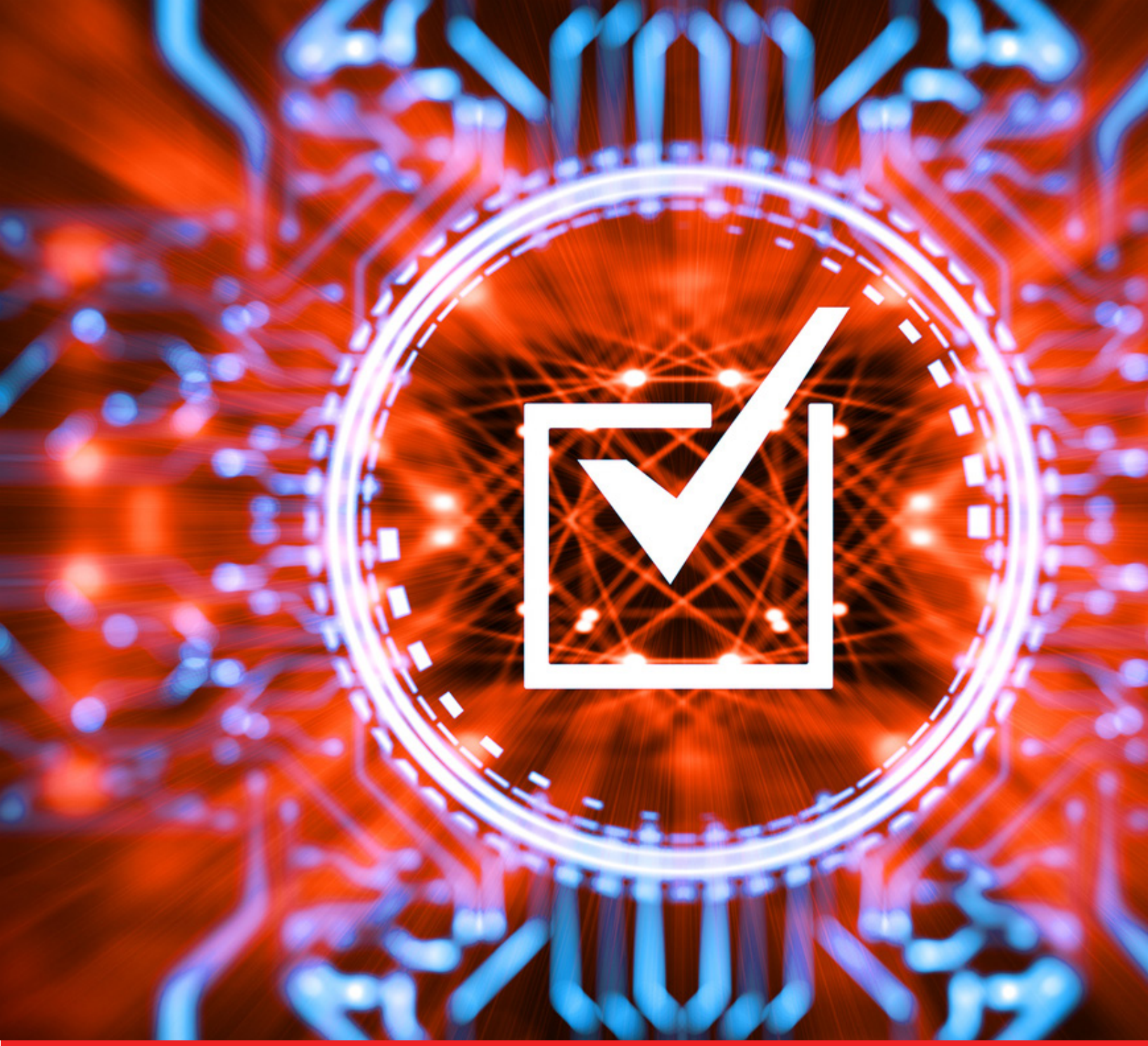
I'll say it again: there is no flashy — and certainly no easy — solution for dealing with the risks inherent in using third-party tools. It's all about covering your basics, doing due diligence and maintenance, and keeping your ear to the ground.

Following these best practices, maybe you can't say "I'm not vulnerable to anything today," but perhaps you can say with confidence "I'm not vulnerable to anything that came out last month." Or "I have 2020 on lockdown." If you can make it that far, and trust that if you have a well-planned process, you will be catching all sorts of problems before they even arise.

Remember: security should enable business, not throttle it. Drag your risk into a window you are comfortable with, and you'll be in a much better position to protect your system.
Even from ninjas.

About the Author

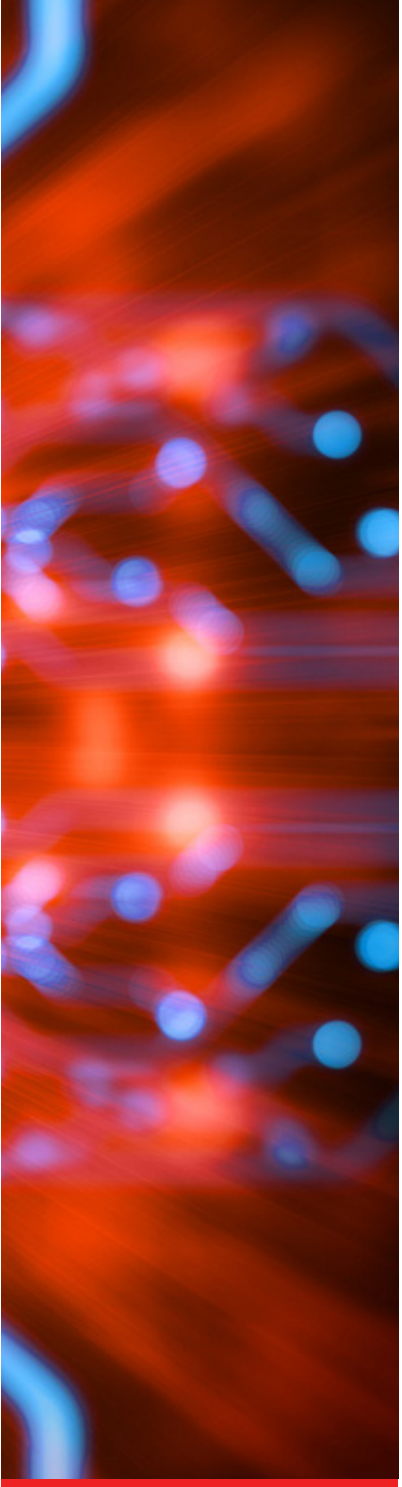
Aaron Kiemele is the Chief Information Security Officer (CISO) at Jamf. With 20 years of experience his background spans a number of industries, with a focus on operational security and compliance.
www.jamf.com



CMMC IS DOA

Why the DOD's Cybersecurity Certification Program Will Never Launch As-Is

By Christopher Paris, Founder, Oxebridge Quality Resources International



There's been much bluster about the DOD's pending CMMC certification program, aimed to have more than 300,000 defense industrial base companies under third-party audits to confirm their cybersecurity controls. This has caused a mix of panic, among defense industry companies who have legitimate questions about costs and rollout, and elation, by consultants who stand to benefit from the new industry created nearly overnight by DOD.

The reality is that CMMC is dead in the water, and cannot launch. Read that again: CMMC is dead.

Despite having been under development since at least 2019, the CMMC program never progressed past vaporware. The CMMC model – or "standard" – is still not completed, and DOD recently announced it intends to release a "major" revision sometime later this year. Next, not a single auditor nor certification body exists that can assess a company to CMMC, and the programs to get assessors and CBs ready have not even been drafted.

Instead, the DOD mandated the formation of the CMMC Accreditation Body, which has spent the past 15 months selling dubious "badges" for consultants, the one part of the scheme that is wholly unnecessary. To repeat: the CMMC-AB wasted nearly a year and a half on the one thing that's in their name: an "accreditation body."

In the interim, the CMMC-AB bungled the basics. In March of 2020, they filed for a CAGE code attesting – under penalty of criminal prosecution – that they were already a tax-exempt organization, when in fact they never filed for tax-exempt status. They then solicited $500,000 "Diamond memberships" in what might have ended as felony tax fraud if the Board hadn't pulled the scam in 48 hours and ejected the Board members responsible. They then failed to trademark their logo, inviting a future filled with pirated CMMC certs and bogus marks. More recently, they failed to update their SAM.gov filing, allowing it to lapse earlier this month.

It does not appear that the DOD contract that mandated its formation is legal, nor will it survive even a minor legal challenge. Criminal investigations are underway, as well as over a dozen other probes. Talks of class-action suits have begun.

Ironically, that's not what will kill CMMC. Instead, it was the even-more-monstrous bungling by the DOD itself.

Early on, DOD dreamed up a plan to marry a CMMI-style "maturity model" concept with old-fashioned ISO certifications. Without any actual accreditation experts to advise them, DOD never realized the two don't mesh. Maturity models are graded systems, sloped and allowing a variety of results based on, well, "maturity." ISO certifications are pass/fail, binary attestations. The system was broken before they ever launched it.

Next, DOD apparently "heard some stuff" about ISO accreditations, and so mandated that the CMMC-AB would become an official accreditation body by obtaining ISO 17011 accreditation for itself. In the ISO scheme, this is managed by an organization called the International Accreditation Forum (IAF), so DOD put in its contract that the CMMC-AB would join that oversight scheme.

The only problem is that the IAF is run by China. Its current president is Xiao Jianhua, the chief executive of CNAS, the Chinese National Accreditation Service. Other CNAS execs perform other duties in various IAF roles.

In the world of commercial ISO certifications, this is not a tremendous problem, although it does cause some headaches which are out of scope for this article. But the arrangement is not a national security risk.

Under the DOD contract, the CMMC-AB would join the IAF's regional body for the Americas, known as IAAC, which operates out of Mexico, because Mexico resides in one of the "Americas," just not the United States Of. It does not appear that DOD realized this bit of geography.

Membership in IAAC will require the CMMC-AB to undergo "peer audits" by foreign nationals from China, Mexico, Brazil, and a host of other countries, in order to verify the CMMC-AB's compliance to ISO 17011. The procedures for these audits are not hidden, and available on both the IAAC and IAF websites for public review. They reveal that these peer audits will require the IAF and IAAC to physically attend CMMC-AB's assessments, allowing foreign nationals to witness – in real-time and in-person – as auditors uncover cybersecurity weaknesses of defense companies, and write up "nonconformities" to get them addressed. Then, additional "office audits" will allow those same foreign nationals to review the corrective actions companies take to close those nonconformities.

The DOD literally handed China a VIP backstage pass to the nation's cybersecurity gaps and lapses.

Worse, under the IAF multilateral agreement, any appeals filed against the CMMC-AB would – if not handled properly by the CMMC-AB itself – eventually be adjudicated IAAC/IAF. If China wanted to throw a wrench in the works it need merely uphold a single complaint, and eject CMMC-AB from the IAF/IAAC roster, stripping it of its accreditation. The CMMC-AB would immediately be in violation of its DOD contract, and everyone would panic.

And obviously, the first company that fails its CMMC assessment is going to file an appeal. In the ISO world, this is a routine occurrence.

The DOD error was entirely avoidable. In September of 2020, I wrote a white paper detailing this threat, and outlining a simple plan to avoid it; instead of relying on bodies like IAF to oversee the CMMC-AB, the role would fall to the DOD itself, and an independent ombudsman. DOD rejected the paper, and pushed forward, insisting they knew better, while the CMMC-AB just ignored it outright. The parties then signed a contract hardcoding Chinese oversight of the US defense industry and went to bed that night thinking that was a good idea.

To be clear: there is no way this survives. Under no possible circumstance will anyone allow the CMMC-AB and defense companies to undergo peer audits by IAF or IAAC. Period.

Congress, along with a number of Inspectors General and agencies, are already examining this remarkably bad idea. The CMMC plan will be scrapped, the CMMC-AB disbanded, and those responsible at DOD will move on to other careers. (In fact, most have left already.)

The only question is what will come from the ashes. Perhaps a new CMMC-AB will be formed, independent of Chinese and Mexican oversight. Perhaps the entire thing will be scrapped and cybersecurity certification will be given to NIST or DIBCAC or DCMA or some other agency. For my part, I will keep proposing solutions, but we need to wait for mature adults who will listen, rather than shameless hucksters selling a future of endless consulting contracts.

But rest assured: the CMMC plan that is being floated now will not survive. Whatever does emerge will be very, very different.

About the Author

Christopher Paris is founder of Oxebridge Quality Resources International, an aerospace quality management consulting firm. He has worked in ISO certifications and accreditations since 1988, and his clients have included SpaceX, Northrup Grumman, and NASA. He is the author of the books Surviving ISO 9001 and Surviving AS9100, and is the creator of THE AUDITOR, a caustic comic strip which eviscerates the ISO certification market. He manages the LinkedIn ISO 9001 Group with over 125,000 members, and can be reached at cparis@oxebridge.com.

East-West Attack Prevention with Secure KVMs

By John Minasyan, Director of Product Management, Cybersecurity Business Unit, Belkin

For the past year, our everyday activities have been confined to the online world, making users more susceptible to cyberattacks. The FBI's Internet Complaint Center has seen between 3,000 and 4,000 cybersecurity complaints each day, a major jump from pre-pandemic, which saw about 1,000 daily.

The public sector saw some of the largest numbers of attacks in history, and government agencies are looking for the best ways to combat cyber threats. A cyberattack can take down an entire system, destroy valuable equipment, leave government agencies vulnerable, and put national security at risk.

According to the 2020 Verizon Data Breach Investigations Report, the government suffered from 6,843 security incidents from 2019 to 2020, 346 with confirmed breaches. While threat origins are numerous, miscellaneous human-based errors lead the pack in terms of cause, according to the report.

Hackers are getting smarter with their solutions and innovating faster. A network breach can be detrimental, but east-west attacks can be even more damaging to networks. This type of attack travels from a compromised host or network to a more valuable one, making it especially difficult to determine where the attacker has been and what they have touched.

In an attempt to protect the most valuable and sensitive information, agencies rely on isolated networks to protect mission-critical data. The most effective solutions implement air-gap networks, ensuring that advanced signaling attacks that may compromise a desktop have no way of propagating to more sensitive systems as there simply is no route from one network to the other.

These air-gaps can still be breached, especially if users share computer peripherals between multiple systems. Embedded memory in these peripherals can be utilized as an unwitting conduit to bridge the air-gap and expose sensitive systems to damaging attacks.

Preserving Air-Gap Isolation

Peripherals can be safely shared without compromising air-gap isolation through the use of secure keyboard-video-mouse (KVM) switching devices. Secure KVMs are certified by the National Information Assurance Partnership (NIAP), which ensures that these secure KVMS are safe for use across security domains on government networks. The latest standard, released in 2019, provides enhanced vulnerability protection while allowing manufacturers the flexibility to address more user pain points.

While KVMs have been around for years, their use and functionality have remained static and inflexible. With the flexibility built into the new NIAP Protection Profile for Peripheral Sharing Devices version 4.0 standard, secure KVMs can now innovate to deliver secure peripheral sharing with an elevated user experience. Secure KVMs will soon be available with peripherals that enhance user awareness and control while eliminating clutter and complexity on the desk. Further, universal video format support will allow the same KVM to be used across multiple deployment scenarios without the need for external audio/video converters or adaptors, minimizing compatibility issues, deployment time and unbudgeted costs.

Government agencies need to implement secure KVM solutions to protect against vulnerabilities at the desktop and maintain air-gap isolation between secure and non-secure networks – but also to enable a productive, flexible workspace. By utilizing solutions that emphasize user experience and prioritize future-ready technology, agencies can deliver critical security with limited compromises for stakeholders. Belkin's 4.0 Secure KVM solutions give government agencies the flexibility to design their environments and equip employees with the advanced functionalities and an advanced user experience.

Investing in the Right Solutions

Security continues to be a high priority for government agencies, as risk of attack increases and the number of attacks grows every day. Secure KVM solutions offer advanced security and functionality for these data systems. By prioritizing air-gap isolation and physically blocking the potential for cross-domain propagation of an attack via shared peripherals, agencies can mitigate risk and provide their operators a highly evolved, effective, and efficient work environment.

About the Author

John Minasyan leads Belkin's cybersecurity business unit focused on solutions to mitigate advanced threats at an operator's desk. Throughout his career, Mr. Minasyan has been at the forefront of advanced technologies and the convergence of IT. Prior to Belkin, his career included leadership roles with companies at the forefront of communication semiconductors and IP video security systems. He serves on the United States' NIAP Technical Committee for Peripheral Sharing Switches and is a member of the US IT Sector Coordinating Council of technology companies chartered with sharing practical cyber defense strategies with industry.

John can be reached online at john.minasyan@belkin.com and @johnminasyan on Twitter and at our company website https://www.belkin.com/cybersecurity.
John Minasyan
Director of Product Management, Commercial Products

Belkin International
121 Theory, Suite 150, Irvine, CA 92617
O +1 949-270-8504
M +1 559-363-5646
T @johnminasyan
S john.minasyan@belkin.com

Your Cloud is Having an Identity Crisis: Why it's happening — and how to deal with it

By Eric Kedrosky, CISO and Director of Cloud Research of Sonrai Security

If you're like most organizations, you haven't dug deep enough to understand the complexities of all the Identities and their interconnected relationships and intricacies in your multi-cloud environment. Even after all the headlines of the past few years where organizations have suffered massive data breaches in their public cloud, there are still some who think that this won't happen to them. They are wrong.

Identity and data access complexity is a ticking time bomb in your cloud. The average organization has more than tens of thousands of pieces of compute, thousands of roles, and a dizzying array of interdependencies and permissions to their data, and it is mostly hidden from view. Your environment is having an identity crisis and you have no visibility into the risks that exist.

The security paradigm changed as soon as you moved to the public cloud. Did you notice? More importantly, have you changed your security strategy to adapt and keep your data safe? In the old days of data centers, the security boundaries were formed by networks and the security stack placed at the borders. In the cloud, this is no longer feasible, manageable, and in a lot of cases, even possible.

Workloads in the cloud are extremely complex. It becomes increasingly challenging to instrument the cloud and send voluminous amounts of alerts to responsible security teams. DevOps need to understand how quickly these workloads fire off and how automation is required for the desired result. Teams need to understand the complexity. The intricacies of rules and regulations demand complexity to reduce risk and increase security. Global restrictions make cloud security even more complex.

In the cloud, Identities, human and non-human, are the new security perimeter. As such, a new approach to security is needed, one that focuses on Identity and data governance. Organizations that have recognized this, and adjusted their strategy, are already seeing the benefits, not just to their security program, but also to their overall business. Let's look at some of the challenges they faced and more importantly overcame.

Organizations Fail to See the Common Identity Blind Spots

Many organizations fail to recognize the most common Identity management blindspots. Let's start with the highly privileged Identities. While not all users enjoy the same level of access across cloud services and resources, some Identities accumulate high levels of privilege due to their various responsibilities. This means they can move in and out of important accounts relatively unchecked. Examples include managers, software engineers, content professionals, members of the finance team, and more - the unchecked Identities.

Another common blind spot is granting elevated permissions to individual users which can cause considerable harm. For example, a user may be able to change system configuration settings, share access with other users, or lift sensitive information that can be sold for profit. As such, it is important to err on the side of restricting access.

Lastly, your organization is too slow in de-provisioning. Further problems can arise when end users, human Identities leave an organization without being properly de-provisioned, increasing the likelihood of a catastrophic data breach. Because non-human Identities can also take on a role like a user, an organization may lose visibility into what can be accessed. IT administrators need to have a centralized system in place to control Identities for rapid provisioning and de-provisioning.

Don't Stumble on Your Lack of Cloud Guardrails

An organization's Cloud Service Provider (AWS, Azure, or GCP) enables guardrails to provide strong preventive and detective governance throughout their environment. Guardrails can be used to control system resources and monitor compliance across accounts, organizations, roles, Identities, and non-human Identities. However, cloud-native guardrails are not enabled by default and can be disabled by system administrators.

Furthermore, these guardrails are often at different stages of maturity and almost always within their own pane of glass, which makes effectively managing within your cloud very difficult. Managing across different clouds - forget about it! Without guardrails in place, organizations are highly exposed to any number of threats, such as data theft or unauthorized access. While guardrails may vary in scope from organization to organization — or even across different cloud providers — they should always be used.

Failing to Protect Non-human Identities

Non-human Identities will go ungoverned if you only focus on human Identities or users in your environment. This is a critical mistake. The majority of Identity and Access Management spend goes towards protecting human accounts. Unfortunately, this means that organizations often overlook the vast number of non-human Identities in their cloud — which is troubling when considering the breadth and depth of access these Identities have. If you are unable to continuously audit and monitor what these are, and more importantly, what they can do, what data they can access, and what they are actually doing, you are running blind and at great risk.

Without a strong Identity security platform in place, it's impossible to know when Identities are misconfigured and being used in malicious ways. Similar to lateral movement from server to server in the data center, hackers can use Identities to worm their way deeper into your cloud — the end result is wreaking havoc by stealing information and/or shutting down critical systems.

The Plan Isn't Working Anymore

As your cloud is embroiled in an Identity crisis, it can steer its way out into a happy, more secure environment. Organizations can close the gap on this Identity crisis with a few simple steps.

Continuous inventorying and monitoring of all human and non-human Identities, plus their effective permissions, is possible. With the right tooling, organizations have the ability to track permissions and provide continuous monitoring within and across their clouds and provide alerts to highlight a risk before it becomes an incident. In parallel, tools can generate when deviations and/or suspicious activity is detected. In both cases, teams can use automation to eliminate the Identity security risks and issues at the speed of the cloud. The end result is a highly resilient organization.

A true Identity crisis usually involves a data breach. So the question remains – do you do something drastic or do you wait for something drastic to happen in your cloud? Proactive, rather than reactive, measures matter more now than ever.

About the Author

Eric Kedrosky is CISO and Director of Cloud Research of Sonrai Security. Eric Kedrosky joined the cloud security software company in February 2020 after 16 years working in the industry. Highlights from his career include working as Director of Security & IT at Verafin, Directory of Information Services & Security at RigNet, and Enterprise Global Xpress (GX) Manager at Inmarsat. Kedosky graduated from Carleton University in Ottawa, Canada with a Bachelor of Engineering with a focus on Computer Systems. He stood out from his fellow students so much that he immediately got hired as a Security Analyst at Nortel. He rose quickly through the company's ranks and left to pursue an interest in business solutions development with Bluedrop Performance Learning, the first online learning network. Eric can be reached online at: LinkedIn: https://ca.linkedin.com/in/erickedrosky
Twitter: @EricKedrosky and at our company website
http://www.sonraisecurity.com

Top Predictions for AI in Cybersecurity in 2021

By Bill DeLisi, CEO of GOFBA

To remain competitive and relevant in 2021 and ahead, cybersecurity vendors must leverage AI and machine learning. It's a necessity because those technologies are both the cause of sophisticated hacking efforts and the viable solution to combat those efforts. They're already in play on both sides of the equation. For example back in 2017, a team created an AI-driven tool that could quickly guess the passwords of around a quarter of 43 million LinkedIn profile accounts. Hackers increasingly use machine learning and AI to circumvent traditional cybersecurity safeguards, especially with increased threats during COVID-19, which puts pressure on companies and technology providers to react with the same tech. As we move into 2021, here are some of the security areas where we can anticipate AI's role to expand and evolve.

AI Integrated into Antivirus and Authentication Systems

AI can play a role with antivirus programs by learning the ways a system should normally operate. Then if a malware program reaches the network and starts accessing various systems, the antivirus programs recognize this as an anomalous action and blocks the program. It's a familiar machine learning pattern of understanding the normal state of a system and then spotting odd behaviors.

On the authentication side, AI can reduce risks and stop intrusions before bad actors get into various systems and cause harm. For example, multi-factor authentication (MFA) programs involve several different factors and user behaviors. AI comes into play with risk-based authentication, where the AI sets risk scores that are based on the login attempt context. Another example, a user who typically logs in from home during business hours would have a different risk assessment than the same user credentials being used at two in the morning from a different IP address. The AI effectively learns what sets of risks are likely to produce the right results (successful proper logins) and then adjusts and improves over time until it can reliably predict an unauthorized login.

Reducing Phishing with Enhanced Intelligence

Into 2021 and beyond there will be an expansion of AI into phishing prevention. In a similar structure to its capabilities with antivirus and authentication programs, AI can also spot anomalies that point to a phishing scheme. These anti-phishing programs look for inconsistencies in email message content and metadata. An AI-informed solution can learn over time how to spot phishing-style language such as urgent requests (respond immediately with your credit card!) that are likely fraudulent in intent. It can also determine spoofed email senders, misspelled domain names, and other tricks found in emails that aren't always spotted by the human. It's a context-based dynamic that also considers if the email is part of a string, and if there's an established connection between sender and the recipient. Providers can add AI on top of traditional authentication tools like SPF, DMARC, and DKIM.

Improving Remote Work Security

Security is a key consideration for every firm that moved to remote workforces during the pandemic. A mobile workforce that can operate from any location with a laptop and Wi-Fi access presents considerable challenges for IT. Workers are exposed to online dangers but secure search engines and communication platforms (such as GOFBA) can help mitigate threats. There is also the risk of "shadow IT" where workers go rogue and pick their own cloud storage or messaging apps instead of the company-approved tools. A training gap also exists, with many workers unaware of the risks their actions pose to company networks and their own jobs. AI can help mitigate many of these risks by improving anti-virus tools and other security programs, and also learning about work from home patterns and then developing contextual risk assessments.

AI and machine learning can improve multiple remote working functions. For example, an AI tool could use the worker's laptop camera to note when someone else is in the room. This could then shut down access to sensitive information or make their screen go blank for a certain period. This feature could be invaluable for workers and companies dealing with compliance regulations that apply to the usage of certain data sets. AI is also used in hiring tools such as applicant tracking systems and other HR functions to better screen people before they're hired. And employee monitoring tools will also use AI to delivery more accurate contextual-based results to management about the employee's daily or monthly activities.

Aiding the Human/Machine Mix

In 2021 and the years ahead, cybersecurity teams should develop a better understanding of AI's capabilities, specifically as they compare to human capacity. Current AI tools are improving, but many are still flawed and do not understand human intuition and motivations. An article in the MIT Technology Review dives deeper into AI's limitations, saying "These shortcomings have something in common: they exist because AI systems don't understand causation. They see that some events are associated with other events, but they don't ascertain which things directly make other things happen. It's as if you knew that the presence of clouds made rain likelier, but you didn't know clouds caused rain."

This year the industry will see more decisions among IT and cybersecurity teams about the ways AI-driven tools can best incorporate human intelligence and decision making. It will promote transparency to the ways AI provides context, showing it doesn't just spit out answers. This is part of the next leap for AI and machine learning, where the tools can "reason" and perform complex "what if" scenarios that are currently out of their grasp but easy for humans.

According to a Capgemini report titled "Reinventing Cybersecurity with Artificial Intelligence," sixty-nine percent of surveyed industry respondents noted AI will be necessary to respond to future cyberattacks. The decision makers know it's needed to thwart threats but integrating AI into various cybersecurity tools remains a challenge. In 2021 and the coming years, hackers will continue to introduce ever-improving AI and machine learning tools, and providers need to stay a few steps ahead by doing the same, but just a little bit better.

About the Author

Bill DeLisi is one of the world's most authoritative experts on cybersecurity. He is currently the Chief Executive Officer, Chief Technology Officer and a founding member of the Board of Directors for GOFBA, Inc. DeLisi has more than 30 years of experience in the computer industry, including holding the position of Chief Technology Officer at several companies. He has worked closely with Microsoft Gold Certified Partners, helping pioneer "cloud" computing and creating security infrastructures that are still in use today. DeLisi is responsible for the development of proprietary technology that serves as the backbone of GOFBA's platform and has over 30 certifications with Microsoft, Cisco, Apple, and others, which includes the coveted Systems Engineer with Advanced Security certification, as well as expert status in Cloud Design and Implementation.

Bill can be reached online at his LinkedIn and the company website is: https://www.gofba.com


EVENTS

CYBERCON LONDON 2021

UNMISSABLE ONLINE EVENT

Managing fraud risk and cyber-security

12TH + 13TH MAY 2021

Led by world's leading experts in the field of cyber security and financial fraud investigations, CyberCon London 2021 is an unmissable opportunity to ensure your business and security systems are up to the challenge of an always evolving cyber threat.

UK business leaders and C-level executives across industries will have a first-hand access to some of the top international experts who will share their insight and expertise in developing effective threat management strategies and solutions to new and unprecedented online/cyber threats that have emerged in the year under a lockdown through interactive Q&A sessions and insightful panel discussions.

WHO SHOULD ATTEND:

- CHIEF TECHNOLOGY OFFICERS
- CHIEF INFORMATION OFFICERS
- CHIEF INFORMATION SECURITY OFFICERS
- IT DIRECTORS
- MANAGING DIRECTORS
- RISK & COMPLIANCE OFFICERS

REGISTER VIA
WWW.CYBERCONLONDON.CO.UK

#CYBERCONLONDON

CYBER DEFENSE TV

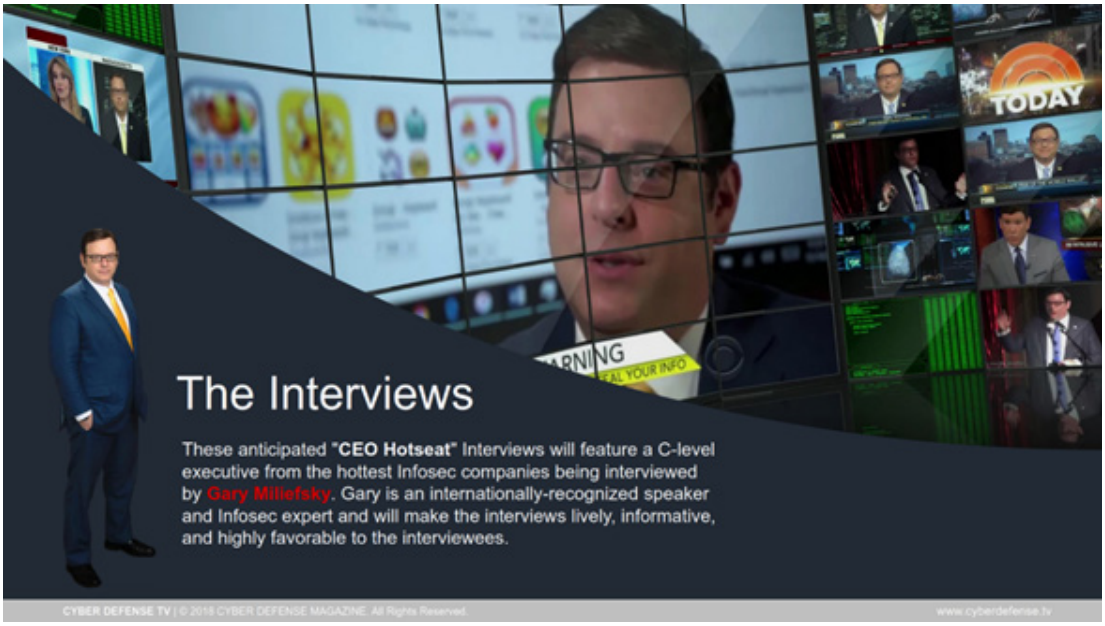
INFOSEC KNOWLEDGE IS POWER

You asked, and it's finally here…we've launched CyberDefense.TV

Hundreds of exceptional interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A new 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.

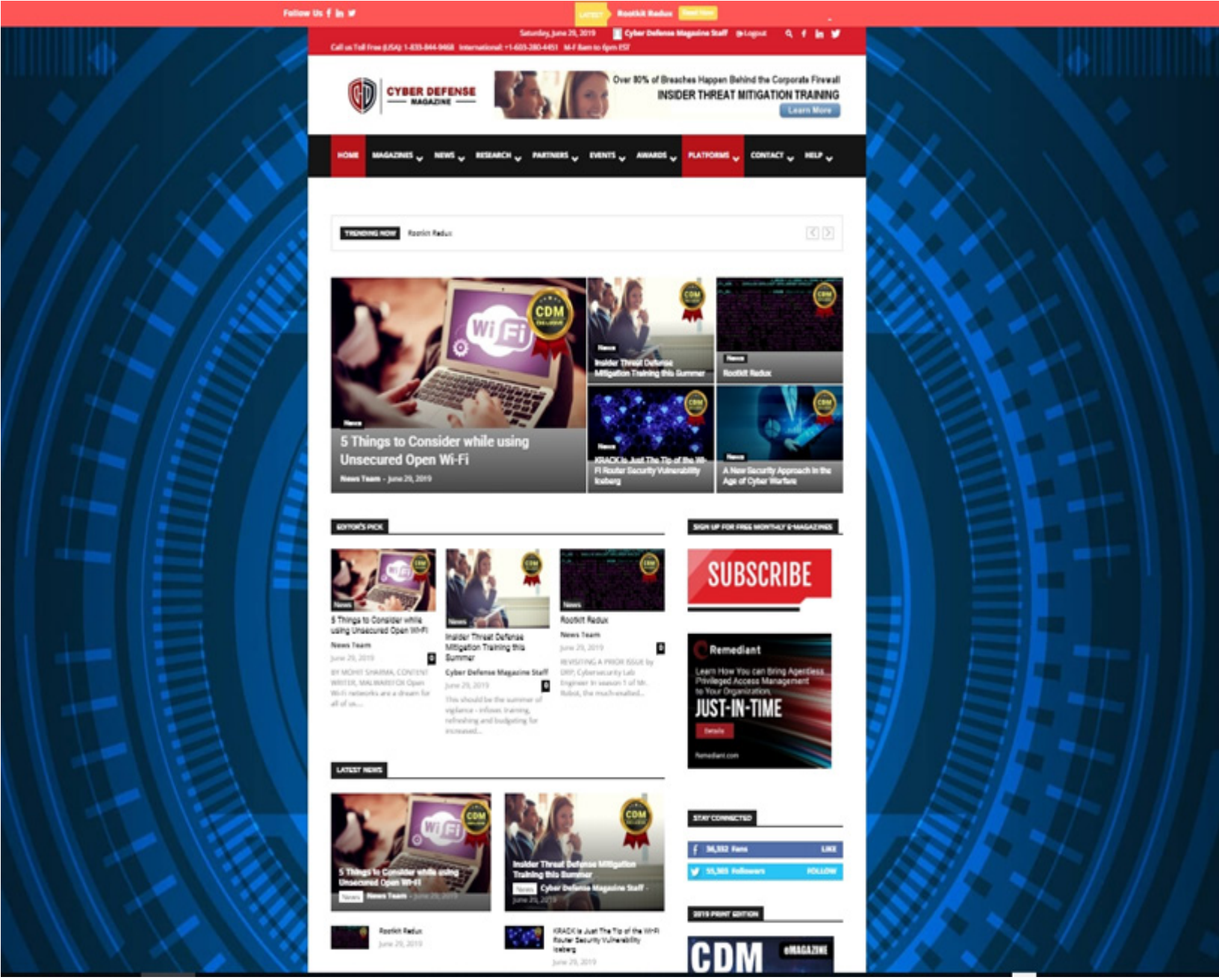
This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on 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: 04/02/2021
Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)



9 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 shooting for 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites and our new B2C consumer magazine CyberSecurityMagazine.com.

Millions of monthly readers and new platforms coming…starting with

https://www.cyberdefenseprofessionals.com this month…

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert

ALWAYS FREE
NO STRINGS ATTACHED

*** with help from writers and friends all over the Globe.**