CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

IN THIS EDITION

MAY 2019

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

65+ Cybersecurity Top Executive Hotseats on CyberDefenseTV.com and more plus CyberDefenseRadio.com is up!

Dear Friends,

We are so hard at work with a humble goal – to be the #1 source of all things InfoSec knowledge – best practices, tips, tools, techniques and the best ideas from leading industry experts. We're on path to make this happen entering our 7th year in 2019 with over 7,000 original pages of searchable InfoSec content. Here are our current results, so far, thanks to your support. We're tracking our results on various independent websites that track keywords across the global internet and here's where we stand today: https://essentials.news/en/future-of-hacking. We also offer our own statistics that you are free to reuse anytime, from this page: http://www.cyberdefensemagazine.com/quotables/. We believe in sharing information and helping educate others with as much open source intelligence (OSINT) and unique, daily updated content as possible.

I'm thrilled to announce after 7 years of prestigious InfoSec Awards during RSA Conference and Global Awards during IPEXPO Europe, we have now just launched Black Unicorn Awards for 2019 which will be given out to only 10 winners during Black Hat USA this August in Las Vegas, Nevada, USA; With some amazing Judges this year, like Robert Herjavec and David DeWalt! Learn more at:

www.cyberdefenseawards.com

With *much appreciation to our all our sponsors – it's you who allow us to deliver great content for free every month to our readers…for you, our marketing partners, we are forever grateful!*

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS

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

From the Editor…

We're seeing a major shift in the way cybercriminals are approaching their exploitation methods – for example, there are attacks using open source intel (OSINT) from employee social media accounts – attacks against social media accounts and more threats against cloud service providers (CSPs).

In parallel, we see new players coming into view that see this as a new opportunity for proactive countermeasures. We've seen new and innovative cybersecurity technologies to help protect critical infrastructure.

Finally, we've seen a lot of solutions for dealing with the major risks in the shift to the cloud including identity and access management (IAM). The market continues to evolve and we'll keep you up to speed on how its shaking out against data theft, cybercrime, cyberwarfare and hacktivism.

Some of these players will be recognized through our Black Unicorn Awards in August so stay tuned.

Please Enjoy This May Edition of CDM!

To our faithful readers,

Pierluigi Paganini

@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

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

WE'RE CELEBRATING

7 YEARS OF EXCELLENCE!

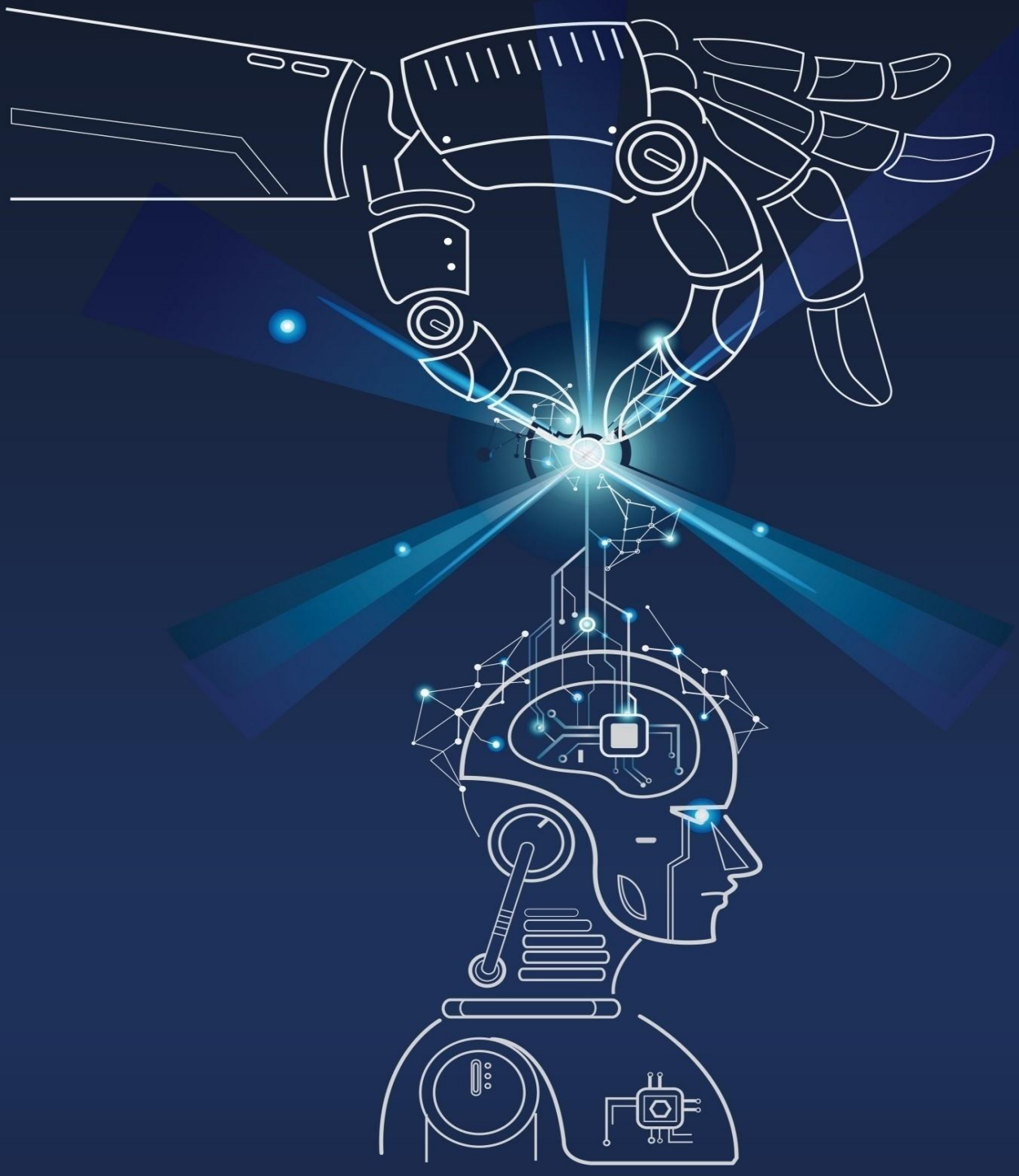
Providing free information, best practices, tips and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS


SPONSORS

InfoSec Knowledge is Power
Free Cybersecurity Resources



www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefensemagazine.com

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

DON'T LET COMMUNICATION BE YOUR POINT OF FAILURE.

The **Vaporstream® Secure Communication Platform** lets organizations securely collaborate with confidence during times of crisis.

Vaporstream eliminates the vulnerabilities of the traditional communication and information sharing channels such as email and standard SMS. Our enterprise-grade, secure and compliant communication platform empowers business continuity and command of any crisis outside of your network, without worrying about information leaks to bad actors, the media or the competition that could impact your reputation or bottom line. Take control of communication during any crisis. **Learn how Vaporstream helps you keep communications secure, compliant and leak free.**

Vaporstream

Visit us at www.Vaporstream.com/security.

New Year, New You,
New File Transfer Solution

2019

Is streamlining and securing your file transfer processes on your 2019 to-do list?
If so, a managed file transfer solution can help!

You might benefit from MFT if:

1. You use traditional methods (e.g., FTP or legacy scripts) to send data.
2. You want to automate your batch file transfers.
3. You need to comply with data security laws and regulations.
4. You want to protect your data with modern encryption methods.
5. You need to easily and securely exchange data with trading partners.

GoAnywhere MFT fits all these needs and more. Start 2019 off right with a new solution that's quick to implement, runs on multiple platforms, and is user-friendly for all.

Try GoAnywhere today!
Download a free 30-day trial of our award-winning MFT solution at
www.goanywhere.com/trial

GO ANYWHERE®
Managed File Transfer

Connectivity with Salesforce, Google Drive, SharePoint, and More...Simplified

Wouldn't it be nice if your file transfer solution allowed for plug-n-play connectivity with the web and cloud applications you use every day?

THIS IS 100% POSSIBLE WITH

GO ANYWHERE®
Managed File Transfer

GoAnywhere is a managed file transfer solution that simplifies how you encrypt and automate your data transmissions. Together with GoAnywhere Cloud Connectors - powerful web and cloud integrations - you can streamline connections with these applications and more:

Dropbox

Google Drive

VOTIRO SECURED.

salesforce

SharePoint

Jenkins

Microsoft Dynamics 365

zendesk

Simplify Your Processes and More with Secure Cloud Integrations

Request a Demo: www.goanywhere.com/demo

Visuality Systems

Protect Your Product From Malicious SMB File Sharing Activities, Upgrade To An

Encrypted SMB VERSION 3

Secured Access To Remote Files

sanernow

Array of tools for Endpoint Security and Systems Management

- ✓ Vulnerability Management
- ✓ Patch Management
- ✓ IT Asset Management
- ✓ Compliance Management
- ✓ Endpoint Threat detection
- ✓ Endpoint Management

secpod

REAL-TIME CONTINUOUS DIAGNOSTICS & MONITORING

SHINE A LIGHT ON THE DARKEST CORNERS OF YOUR NETWORK

STIGs & Configurations

Continuous audit of policies & controls.

Threats & Vulnerabilities

Real-time discovery of Threats & Risk.

Asset Discovery

Automatic inventory & tracking of assets.

User & Entity Behavior

Monitoring of risky & unsanctioned activity.

Looking for the information you need to **Identify Risk**, **Direct Remediation**, and **Document Results**?

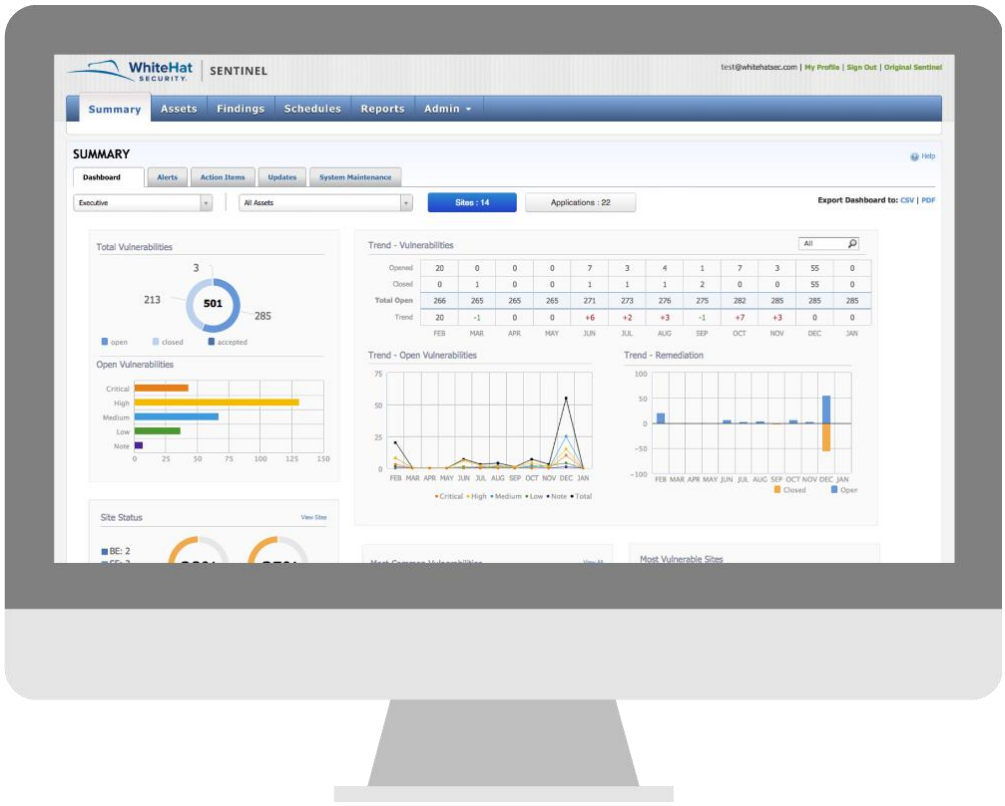
Look no further...

Get meaningful, actionable, and repeatable data, in real-time. AristotleInsight® is the world's first Continuous Diagnostics & Monitoring (CDM) Platform to bridge the gap between security frameworks and real-world IT Technologies.

Get the information you need, when you need it, with AristotleInsight.

AristotleInsight®
— Identify | Remediate | Document —

AristotleInsight.com | Call us at 866.748.5227



Your website could be vulnerable to outside attacks. Wouldn't you like to know where those vulnerabilities lie? Sign up today for your free trial of WhiteHat Sentinel Dynamic and gain a deep understanding of your web application vulnerabilities, how to prioritize them, and what to do about them. With this trial you will get:

An evaluation of the security of one of your organization's websites

Application security guidance from security engineers in WhiteHat's Threat Research Center

Full access to Sentinel's web-based interface, offering the ability to review and generate reports as well as share findings with internal developers and security management

A customized review and complimentary final executive and technical report

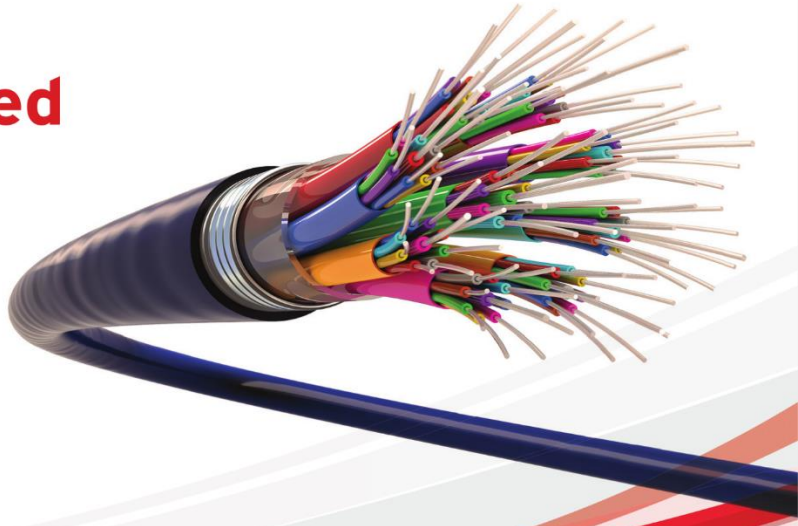
Click here to sign up at this URL: https://www.whitehatsec.com/info/security-check/

PLEASE NOTE: Trial participation is subject to qualification.

TREND MICRO

POWERED BY XGen SECURITY

Detect and prevent breaches at wire speed



Your enterprise is in the crosshairs of the increasingly complex array of ransomware, advanced threats, targeted attacks, vulnerabilities, and exploits.

Only complete visibility into all network traffic and activity will keep your network security ahead of today's purpose-built attacks which bypass traditional controls, exploit network vulnerabilities, and either ransom or steal sensitive data, communications, and intellectual property.

Trend Micro Network Defence detects and prevents breaches at wire speed anywhere on your network to protect your critical data and reputation.

NSS LABS RECOMMENDED

Proven capability

Trend Micro TippingPoint:
"Recommended" Next-Generation Intrusion Prevention System and 99.6% security effectiveness.

Trend Micro Deep Discovery:
"Recommended" Breach Detection System 4 years in a row and 100% detection rate

Industry leading threat intelligence

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

Please get in touch:
Bharat Mistry, Principal Security Strategist
Bharat_mistry@trendmicro.co.uk

www.trendmicro.co.uk/xgen-cyber


ARTICLES

5 Reasons Why Cloud Security Is Important For All Businesses

With practically every business running on some kind of a cloud network and database, securing the cloud has never been more important, here are the most important reasons why.

By Jeremy Stephens,Cyber Security And Outreach Specialist, Power Consulting

Photo: Pexels

With 96% of all enterprises in the U.S. Using some form of cloud computing, it's clear that this technology has experienced a rapid proliferation in the past few years.

Cloud computing helps organizations of all sizes operate at scale, decrease their capital overheads, and assist in managing IT infrastructure.

Depending on your needs, there are several different types of cloud deployment you can consider. These are grouped together in three types:

1. Private Cloud

A private cloud is restricted for use within a specific organization. The infrastructure and resources aren't shared with other companies. Such types of cloud deployment are expensive to set up but offer more customization and security.

2. Public Cloud

A public cloud is managed by an external, third-party provider. Space on this cloud server is 'rented' out to organizations, but the external party is responsible for security, maintenance, and other forms of upkeep.

3. Hybrid Cloud

As the name suggests, hybrid cloud functions as a combination of both private and public ones. It's suited for organizations that want both rapid scalability coupled with top-tier encryption.

But moving to the cloud doesn't come without its own set of security challenges. Let's investigate why cloud security is important for all businesses.

Guard Against Security Breaches

The cost of an average security breach for a company is a cool $3.8 million.

This figure rises to $7.9 million for American companies with an average time of 196 days for detection of the breach in the first place.

Data security on the cloud is important because you're no longer in total control. If, for example, you choose to run your applications on either a public or hybrid cloud, you're effectively putting your trust in a third-party.

This means you must stay on top of things and ensure that your cloud computing provider understands this responsibility. While it is certainly in the provider's best interest to ensure top-tier security for long-term business prospects, you must, as the client, also go the extra mile.

Manage Remote Work

One of the benefits of using cloud computing is the sheer accessibility of data. Your critical applications can be accessed by employees from anywhere in the world. This results in flexible work arrangements and the possibility to hire staff from all around the globe.

However, the downside to this arrangement is that employees might not adhere to cybersecurity best practices.

If they're working from coffee shops, for example, they're using public WiFi to access the web -- this practice entails an inherent security risk. They might also use personal laptops and phones to carry out their tasks, which means they're more susceptible to malware and phishing attacks.

New malware variants for mobile increased by 54 percent in 2017 according to Symantec's Internet Security Threat Report, so this is a real threat. If a malicious virus enters your system, it'll be hard to contain the damage.

Ensure Disaster Recovery

One of the tenets of business continuity planning is having a comprehensive disaster recovery plan in place. Disaster can strike at any time, be it fire, flooding, or other natural causes.

This could wipe out all of your data. Unless you've safely secured and protected your data, you could, potentially, be at risk of at a total standstill. That's the last thing your customers will want to hear, so the ensuing loss of confidence could be a death knell for your business.

Comply With Regulations

Data protection standards like HIPAA and GDPR are rules that businesses must take seriously –- otherwise, they will incur the wrath of regulators.

These standards were put together to ensure the integrity and security of customer data. At the end of

the day, if the customer data stored on the cloud is compromised, it's you who will have to answer to the regulator.

You can't simply pass the blame on to a third-party vendor (your cloud computing provider in this case) and expect little to no retribution.

Highly-regulated industries such as banking, finance, health, and insurance, legal already have exacting standards in place. The importance of cloud security multiplies in these sectors because of all the risks involved. Sure, a data breach will damage your business reputation and brand, but you'll also be held accountable by external parties.

Eliminate Weak Links and Build Access levels

40 percent of organizations using cloud storage accidentally leaked data to the public. This had compromised their business integrity and gave their competition a leg up.

These leaks weren't a result of malicious intent; rather, they were a result of poor security best practices. One best practice of cloud security is enforcing access controls on employees by just limiting access to data only to those individuals who need it.

This makes it much harder for hackers to infiltrate and prevents errors that lead to data leaks.

Conclusion

When it comes to managing and assessing your cloud technology, there are several things to consider.

Of course, the general service levels such as uptime and speed of data transfer are key, but security cannot and should not be dismissed. In this post, we highlighted the key reasons why cloud security is important for all businesses.

As more businesses shift to the cloud, security will become even more important because it'll be the only way hackers can potentially infiltrate a company's defenses.

About the Author

Jeremy Stevens has spent over half a decade working in the tech industry. Besides learning new things about software and IT, one of his passions is writing & teaching about technology. He is working with Power Consulting and helps produce and edit content related to IT, covering topics such as hardware & software solutions for businesses, cyber security, cloud technology, digital transformation, and much more.

8 Cybersecurity Practices In Health IT Domain That Every Company Should Learn From

Exploring the Cyber Vulnerabilities in Digitized Healthcare Space & Finding the Ways to Fix Them

By Anubhuti Shrivastava, Content Crafter, Arkenea

Cybersecurity is a shared responsibility, and it boils down to this: in cybersecurity, the more systems we secure, the more secure we all are. We are all connected online and a vulnerability in one place can cause a problem in many other places.

- Jeh Jhonson American Lawyer & Ex Govt.Official

Digitization has made the healthcare industry much more streamlined and organized. But data security and digital safety are still two major concerns for the medical sector. As per Cybersecurityventures, ransomware harassments on medical organizations will increase fourfold by 2020.

This is an alarming revelation which has to be addressed immediately by the healthcare sector. But safeguarding confidential health-related data of the patients and keeping IT systems intact isn't easy for medical enterprises.

What Can Be The Biggest Data Breach For The Clinical Industry?

Hospitals and medical organizations deal with Protected Health Information (PHI) and health insurance data of the patients. Any incidence such as unauthorized account access, malicious hacking, system bugs, etc. which cause a loss of this data can be considered as the major data breach for that healthcare entity.

Who Can Be Held Responsible For Medical Cyber Attacks?

Hackers are the criminal behind the majority of healthcare cyber assaults. Moreover, insiders from a particular clinical organization also fulfil their malicious purposes by illegally accessing restricted accounts and data.

What's The Current & Future State Of Cybersecurity In The Healthcare Sphere? Is it getting vulnerable?

As per the data offered by the Impact of Cyber Insecurity on Healthcare Organizations study (2018) showcased on helpnetsecurity revealed that clinical enterprises experienced multiple data breaches in the past years. Also, they have compiled a few key trends predicting the major reasons why the security stakes of PHI are high.

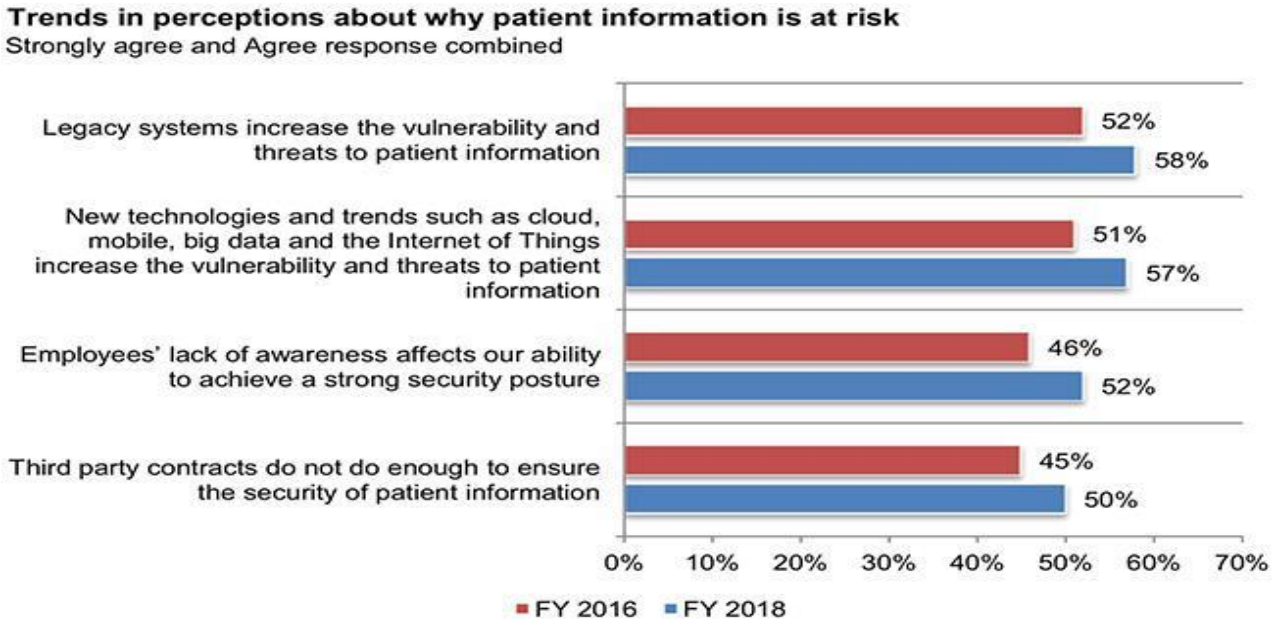


Image Source:

https://www.helpnetsecurity.com/images/posts2018/ponemon-032018-1.jpg

Clearly, this isn't acceptable and the main reasons why the clinical industry is getting even more vulnerable to cyber-attacks can be:

I. Slow approach and ignorance to maintaining and strengthening cybersecurity.

II. Bring Your Own Device (BYOD) policy is on the rise.

III. Internet-based consultations, IoT clinical devices, and integration with multi-cloud SaaS or IaaS environments.

IV. IT systems that are decentralized and proliferation of remote care services.

V. Amplified M&A activities in the medical setup.

As there is a consequence to every incident, healthcare organizations have to bear hefty costs for coping up with these violations. Also, there are rules where the government can penalize such setups and ban their license. So, what should be done with this problem which is getting even more difficult to fix? Let's find out.

What Are The 7 Cybersecurity Practices In Health IT Domain With Which Data Breaches Can Be Stopped?

After familiarizing with the state of cybersecurity in the medical industry along with the major reasons and effects, let's explore how medical enterprises and healthcare providers can get rid of these attacks. Here are eight best practices to help you avoid healthcare data loss and cyber-attacks.

1. Deploy Secure Software Solutions & Ensure Data Protection with Encryption & Automated Updating

The tech-driven landscape has made healthcare organizations aware of tips to hire developers who can build custom-fit software products. These tech platforms streamline complex clinical workflow and automate mundane processes. Electronic Health Records (EHR), practice management suites, medical billing solution, tools for automating scheduling and booking of appointments, etc. are a few of such digital systems.

These platforms deal with confidential health-related details of the patients as well as their personal info such as names, contact numbers, and email addresses. For keeping the data intact it's mandatory to ensure end-to-end encryption with integrating industry standard algorithms.

But be careful to maintain a backup plan to retrieve data safely in case you decide to cease using a particular software. Also, automate the process of patching and configuring these software solutions so that there are no loopholes which can become a boon to cybercriminals.

2. Make Sure To Train Your Staff Properly

In the words of James Scott who is a Sr. Fellow from Institute for Critical Infrastructure Technology, "Hackers find more success with organizations where employees are under appreciated, overworked and underpaid. Why would anyone in an organization like that care enough to think twice before clicking on a phishing email?"

It's a bare truth as your clinical staff is the biggest asset to your healthcare business. In addition to offering lucrative packages, you have to train each one of them so that they can learn how to work in sync with security protocols.

Organize a cybersecurity education program for contractors as well as your employees. Apart from offering primary training, the program must also make them aware of the latest trends in the cybersecurity landscape.

3. Restricted Access to Medical Systems

You should not keep all your clinical solutions accessible to everyone. Limit their usage by giving access to only authorized people for whom the platform is absolutely necessary. Also, keep all the sensitive data at a centralized repository and incorporate a role-based access method.

This will allow your employees to access only those details which are mandatory for them to perform a particular task. Keep track of data access and be cautious about strange or suspicious activities.

Moreover, leverage advanced technologies such as threat intelligence powered by AI and ML in healthcare systems in order to spot irregularities and share it quickly with the entire network. Also, keep track of all IoT medical devices within your organization. Such devices are vulnerable to hackers and a multitude of malware can easily make your confidential data public. So, it's better to monitor the usage of these devices at regular intervals of time.

4. Be Vigilant Towards Your Telemedicine Platforms

Telemedicine is entirely dependent on technology where your medical practitioners use tech-driven communication platforms and digital tools for storing and retrieving of PHI for remote consultations.

Telehealth systems are very convenient for patients located at distant places where it's almost impossible to get medical aid. But at the same time these platforms provide cyber criminals with a gateway for entering your private setup and crack code to fulfill their malicious purposes.

5. Do Not Ignore Common Identity & Access Management Practices

Passwords created by your staff to access medical systems can be vulnerable to allow hackers peep into your restricted network. To prevent hackers from cracking the code integrating a single factor authentication strategy is not a good idea.

This will make difficult for your staff to remember numerous passwords. So, train your staff to keep strong passwords which are tricky to guess. Also, allow them to keep them changing at regular intervals of time.

6. Leverage Mobile Application Management (MAM) Solution to Fight against Cyber Threats

Employees use their own smartphones for accessing multiple apps related to their work. In such a case it's good to implement a BYOD policy. But make sure to use a Mobile App Management (MAM) system to help you in keeping these apps secure. Moreover, keep an eye on healthcare mobility trends and incorporate a robust enterprise mobility management (EMM) solution which can let you stay ahead of the latest tech trends in the clinical industry.

7. Maintain Compliance with HIPAA Technical Safeguards

HIPAA has specified rules which healthcare organizations have to follow for keeping PHI safe and sound. This is why you must be aware of HIPAA standards and necessary digital certificates to keep data secure.

You take help of HIPAA in building an incidence recovery plan. OnPage is a messaging platform built in compliance with HIPAA rules. It can be used to let employees exchange messages containing PHI securely. The plan can help you in recuperating as well as maintaining security in case of an emergency. It can help you in structuring your response and coming out of the crisis easily.

8. Get Rid Of Unwanted Systems & Limit Access to External Platforms

In order to protect your medical data, it's important for you to remove unwanted accounts, software solutions, and browser plug-ins. Also, you must restrict your staff from accessing chat platforms and social media channels on their work machines. Moreover, limit access to doubtful online platforms and external ports such as USBs.

Cybersecurity is one of the biggest priorities for medical organizations. But with keeping the above factors in mind you can develop a secure environment with necessary tech tools to keep PHI safe. Don't rush but consult with an industry expert who can help you in creating and implementing an effective security strategy.

About the Author

Anubhuti Shrivastava, Content Crafter, Arkenea. Anubhuti Shrivastava is a content crafter at Arkenea and Benchpoint. She is passionate about writing articles on topics related to design and the software development industry. Anubhuti can be reached online at anubhuti@arkenea.com and at our company website https://arkenea.com/

SOAR: The Key to Building a Trustworthy Iot

By Cody Cornell, founder CEO, Swimlane and Trent Hein, co-CEO, Rule4

Gadgets and devices connected through the internet of things (IoT) are infiltrating every aspect of our daily lives. From our personal spaces to our businesses, the easily deployable control and sensor technology promotes healthy living, staying connected, improved operational efficiencies, unmanned control and so much more. With giant corporations such as Amazon, Google, Microsoft, and others investing billions of dollars in the IoT space, it's apparent the IoT is changing our lives and the future of business.

Digital transformation has spurred a modern-day industrial revolution as organizations strive to achieve better productivity and management of processes and assets. The rapid proliferation of network-connected devices has created opportunities for smart analytics and machine learning, predictive maintenance, remote monitoring and increased quality management.

In fact, according to a 2017 forecast by Gartner, the number of IoT devices in use will grow to a staggering 20.4 billion by 2020. This rapid escalation is creating a more collaborative, productive and profitable opportunity for information sharing across organizations, which comes with a bevy of both positives and negatives.

Industrial Internet of Things

IoT extends well beyond smart devices in the home and into business/industry. Often called the industrial internet of things (IIoT), this specialized area of the IoT landscape is rapidly growing. From facilities management systems (i.e., HVAC, lighting and access control) and industrial process control systems on factory floors to network-connected treadmills at the gym and on-mountain pass readers at ski resorts, organizations are increasingly deploying embedded devices throughout their networks. Each of these devices can be either a source of data about the environment (including, in some cases, consumer usage patterns) or a way to control a component of the environment.

Whether it's malicious outsiders or employee sabotage, the stakes are much higher in the industrial internet of things, where business continuity and personal safety are both at risk. And the rapid increase in IIoT devices has expanded the attack surfaces and threat vectors the cybersecurity industry is facing on a daily basis.

IIoT Cybersecurity: A Great Concern

Cybersecurity is not always considered as a top priority during an IIoT product's design phase. Because the IIoT is a burgeoning market, many product designers and manufacturers are more concerned with rapidly getting their products to market, instead of taking the necessary steps to build cybersecurity in from the start. From default passwords to a lack of computing resources necessary to implement effective cybersecurity, many IIoT devices do not or cannot offer adequate cybersecurity protection features.

As a result, bad actors are scanning for IIoT vulnerabilities at a frenetic pace. In fact, according to "The CEO's Guide to Securing the Internet of Things," experts have seen a dramatic 458 percent increase in IoT vulnerability scans against devices since 2013, with scans representing adversaries looking for weaknesses in your network defenses.

While the analysis and distribution of collected information and data is essential for device developers and manufacturers to derive predictive models, managing the overwhelming amount of data remains a privacy concern as well. The expectation of the public is when companies handle data, they will handle it securely. Unfortunately, as recent high-profile examples have illustrated, that notion is not aligned with reality.

Today, the IIoT focus is primarily on integration and convergence across industrial verticals. As such, implementing a robust cybersecurity program for IIoT requires a complicated combination of architecture, technical and integration controls as well as adaptation of traditional cybersecurity platforms. And while executing a credible approach to cybersecurity is one thing, the ongoing operational management of authentication credentials and operations, especially for large deployments of non-homogenous devices, is equally important.

Automation

Traditional cybersecurity does not always work with IIoT device deployments. For example, IIoT platforms struggle to verify the authenticity of 10,000 IIoT devices when they don't have associated users to enter a user name and password. A major challenge is keeping IIoT devices updated and secured throughout their lifecycles.

As IIoT device adoption increases, automation becomes an essential component of cybersecurity. Automation is crucial when you think about the vast number of connected devices and applications in our daily lives. Because it's impractical to manage the configuration of 10,000 devices manually, we need to step out of the traditional IT mindset that a human is going to "touch" a device to harden it from a

cybersecurity perspective. Automation ensures consistency and allows the operational status and cybersecurity profile of every connected device to be known.

Security Orchestration, Automation and Response

While security orchestration, automation and response (SOAR) solutions might traditionally be marketed for enterprise IT environments, cloud computing environments that support IIoT devices pose similar privacy and cybersecurity challenges. SOAR solutions can be easily applied as a centralized way to manage a fleet of IIoT devices to ensure that they are always in their best possible state from a cybersecurity perspective.

SOAR solutions can also help with the tedious chore of fleet inventory management, identifying new devices as they come online and deploying appropriate cybersecurity hardening steps. Additionally, SOAR supports a number of key functions in the security operations center (SOC) to help organizations work smarter, respond faster and strengthen their defenses.

Automation enables cybersecurity teams to work smarter by executing previously time-consuming actions across the IIoT environment in seconds, turning what could be impossible into an easy task. A SOAR platform can provide orchestration integration across applications and APIs, enabling cybersecurity professionals to connect and coordinate complex workflows across teams and tools. Events can be aggregated and escalated to cases, which makes them easy to track, then cybersecurity teams can rapidly triage those incidents in an automated, semi-automated or manual fashion. SOAR dashboards combine all the critical information needed to understand the current state of cybersecurity operations and help SecOps teams increase situational awareness and drive efficient communications.

In many IIoT environments, there are tangible life-safety risks where managing cybersecurity though SOAR solutions becomes essential. Consider failing runway lights in an airfield as an example. As an airline pilot prepares for landing, he and his crew don't have time to prioritize alerts to understand what's going on, and nor does air traffic control. Consequently, there must be a system in place that automatically restores those lights so that he can land the plane safely. SOAR platforms provide a highly integrated, automated response that addresses these types of situations.

While the convergence of IT and IIoT networks has created a number of challenges for cybersecurity teams, automation and orchestration technologies have the potential to enable cybersecurity operations professionals to respond to the inevitable challenges ahead. The benefits of SOAR include consistent execution of complex workflows comprised of human and machine-driven actions, as well as an auditable system of record for all these processes, providing the basis for analytics and improvement in the rapidly growing IIoT enhanced world.

About the Authors

Cody Cornell is the CEO of the Swimlane. He is responsible for the overall strategic direction of Swimlane and their SOAR platform. As an advocate for the open exchange of security information and deep technology integration, he constantly strives to enable organizations to maximize the value of their investments in security technology and staff. Cody began his career in the U.S. Coast Guard and has spent 15 years in IT and security including roles with the U.S. Defense Information Systems Agency, the Department of Homeland Security (DHS), American Express and IBM Global Business Services. He has also had the pleasure of presenting at information security at forums such as the U.S. Secret Service Electronic Crimes Task Force, the DHS Security Subcommittee on Privacy and National Public Radio. Cody can be reached online at cody.cornell@swimlane.com, @codycornell on Twitter and at our company website http://www.swimlane.com/.

About Swimlane

Swimlane is at the forefront of the growing market of security automation, orchestration and response (SOAR) solutions and was founded to deliver scalable and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane's solution helps organizations address all security operations (SecOps) needs, including prioritizing alerts, orchestrating tools and automating the remediation of threats—improving performance across the entire organization. Swimlane is headquartered in Denver, Colorado with operations throughout North America and Europe. For more information, visit www.Swimlane.com.

Trent R. Hein is Co-CEO at Rule4, a boutique professional services firm specializing in cybersecurity and emerging technology. A serial entrepreneur, Trent is passionate about building businesses that have a positive impact on employees, clients, the community, and the world. Bedrock to all his ventures is helping clients maximize their IT investment in the areas of security, performance, and availability. Trent holds a B.S. in computer science (CS) from the University of Colorado at Boulder. He is a co-author of the Unix and Linux System Administration Handbook, currently in its fifth edition. Learn more about Trent at Rule4 or find him on Twitter @trenthein.

About Rule4

Rule4 is a global professional services firm that provides practical, real-world knowledge and solutions. Having the right expertise available at the right time is essential, and we're here to help make that a reality. Rule4 provides cybersecurity and emerging technology expertise for every organization. We follow the spirit of Asimov's fourth rule as we help organizations apply technology in efficient, secure ways that benefit and protect humankind and our planet. Rule4 has Certified B Corp Pending status, which means we put people before profit, always.

Blockchain and Cyber Security: Wary Courtship, Or Marriage Made in Heaven?

By Dr. Kevin Harris, Program Director, Information Systems Security and Information Technology Management, American Public University System

For the last several years, perhaps the hottest technology – certainly the one attracting the most attention and investment, if the number of start-up companies focused on the technology is any indication – is blockchain. Given its roots are in cryptography and security, the technology today is increasingly viewed as having a potentially significant role in the development of industry-specific cyber security defenses and systems.

Indeed, on the one hand, blockchain has moved beyond the proof of concept stage, and is showing it has the potential to be a positive disrupting technology in cyber security for a wide range of industries and use cases. At the same time, blockchain has an opportunity to ensure that a secure computing environment is available for a wider segment of the global population.

On the other, blockchain remains in the capacity-building stage: a supporting ecosystem including trained IT professionals, supportive technology, and educated users which must be expanded before we'll see widespread adoption. In this way, the current status of blockchain in cyber security is similar to the position of electrical vehicles before chargers were common place and automotive repair businesses had technicians trained with the new technology.

Opportunities and Challenges for Block chain in Cyber Security

While some argue that the possibility for anonymity is blockchain's most significant benefit, its ability to address all components of the "CIA triangle" (confidentiality, integrity, and availability) is what truly distinguishes the technology. Blockchain's ability to securely save and transmit encrypted files via its chain of digital blocks, gives users the confidence their data has remained confidential, and has not been

altered. And with the decentralized distribution of data, blockchain ensures authorized users have access to data regardless of device or location.

Given that promise and potential, the number one challenge to blockchain adoption will continue to be user acceptance. While the technology has been and continues to be proven effective and efficient in certain applications, its acceptance as a viable, or even central, method is far from certain. A useful lesson here can been seen in the use of biometrics. While biometrics has provided increased security -- especially when implemented as part of a multifactor authentication strategy – it was never fully adopted because of low levels of user acceptance. That said, one advantage blockchain has over biometrics is this: the privacy concerns many have had concerning the potential compromising and malicious use of personal biometrics will not be there with blockchain technology.

Block chain: A More Inclusive Technology

Technology overall has continued to create digital divides between various populations. Security implementation has often widened this gap by requiring implementation in software or hardware. As efforts to protect critical infrastructure components of organizations and nations solutions have been developed to mitigate ongoing threats, investments of resources including financial and personnel are often required to secure sensitive data. . Biometrics is one example of an implementation requiring the acquisition of expensive resources – in this case, biometric readers. Other efforts including PKI certificates require the purchase of certificates or the development of an internal key infrastructure. In these cases, those who could not afford to invest resources in innovative security technologies are at a greater risk of being compromised.

Ironically it is the populations who are at a greater risk which often have the most to lose in the event of a breach. Developing nations in the early adoption stages that experience a disruption could be affected in multiple areas. Confidence in the project could be devastated, leading to reduced support of the initiative. Or, attackers could gain access to a wealth of information that could be used again the nation for years to come.

Individuals in underserved populations often lack the resource to protect personal devices with additional security measures beyond their operating systems. With lax security practices in place, individuals' personally identifiable information is at risk as services are performed online including: banking, accessing of medical records, utilization of governmental services, and engagement of social networks. Other populations that may access sensitive information from multiple locations are transient, including college students, homeless individuals and frequent leisure travelers. Transient populations often use common use machines in libraries and hotels that may be vulnerable.

That's where the promise of blockchain plays a role. Block chain technologies and implementations will allow secure computing to take place without the resource investment previously required. The ability to provide a higher level of cyber security to a large community may allowindividuals and nations to secure valuable digital assests while decreasing the number of machines a hacker can potentially exploit -- and ultimately, lessening the attack vector.

The Future of the Relationship

This year will see blockchain's remaining mystique elbowed aside. As business users and consumers alike are introduced to scenarios where blockchain is utilized or discussed, the technology will inevitably be viewed as a legitimate building block and service enabler. That changed viewpoint, in turn, is likely to lead to higher levels of user confidence, training provider interest, executive buy-in, and inclusion in many organizations' IT strategy and design.

Whether and how that increasing user acceptance will apply to the cyber security sector remains to be seen – but the use of blockchain in cyber security appears to have a bright future, as evidenced by a look at a few potential use cases. In healthcare, blockchain has the potential to revolutionize the sector in a way that probably was not anticipated with the advent of electronic medical records. Medical records can be securely accessed via private node blockchain and accessed by any medical provider. Similarly, in higher education, institutions could use blockchain technology to provide fast, secure access to transcripts. And for businesspeople and consumers who have email addresses – which is to say, just about all of us – blockchain can better protect and secure our email communications, which today are commonly not encrypted.

The bottom line for blockchain and cyber security? The relationship seems to be moving beyond wary courtship and toward the altar, but a bit more dating and time may be required before the wedding invitations are mailed.

About the Author

Dr. Kevin Harris is the Program Director for Cybersecurity, Information Systems Security and Information Technology Management, and serves as the alternate Cyber Center Director at American Public University System. He has more than 20 years of experience in the information technology field with positions ranging from systems analyst to CIO. He performs research on the digital divide and works to ensure a trained cyber workforce in the country. He earned his Bachelor of Science degree in Computer Information Systems from Lincoln University in Missouri; his Master of Science degree in Computer Management Information Systems from Southern Illinois University-Edwardsville; and his Doctorate of Business Administration with an emphasis in Information Systems from Argosy University. Kevin can be reached online at KHarris@APUS.edu and at the American Public University System website, www.apus.edu

Simplifying Cybersecurity Deployments with Automation

By Peter Baumbach

Security is a whole lot like quantum mechanics. It's rife with uncertainty and you can't observe your infrastructure without affecting it. Following this analogy, it's vital to have a system that can cut through the noise and signal to provide value. Today I'm going to take a look at how different types of tools can impact an environment and how to ease that burden. Since we need some kind of tooling to monitor the environment, let's think about the different types: passive and active, each of which could operate on the network, host, or platform layer. Let's talk a little bit about those in general and then we'll take a look at how Alert Logic approaches in the cloud, specifically AWS to streamline and simplify deployment of security tools.

Passive Scanning

Examples of passive methods are SPAN (switch port analyzer) port traffic monitoring for NIDS (network intrusion detection systems) or collection CloudTrail logs from AWS. In both of these examples, some initial configuration is required, but the ongoing impact and maintenance are typically minimal. The big advantage with passive tools is providing a rich dataset for detective controls and a low likelihood of breaking anything.

Active Scanning

WAF's (web application firewalls), traditional firewalls, VA (vulnerability assessment) scanners and IPS (intrusion prevention systems) are active solutions. You either need to set up an appliance or use a cloud-based solution to filter traffic or run scans. An inline technology will either send network traffic through one path on to its destination or drop it. Inline technologies are great blocking known-bad traffic but have the habit of getting into trouble in production with false positives on gray area traffic.

Host-Based Security

Finally, let's investigate host-based tools. With a host-based tool, you are putting a piece of software—an agent—on a host such as a virtual machine or a container. Agents can do all sorts of things like vulnerability detection, log collection, FIM (file integrity monitoring), and more. Agents can be either active

or passive. For example, an agent could simply collect log data, or it could actively isolate a host. While they can do all sorts of cool stuff, there is a huge variance on ease of deployment and impact on the monitored host.

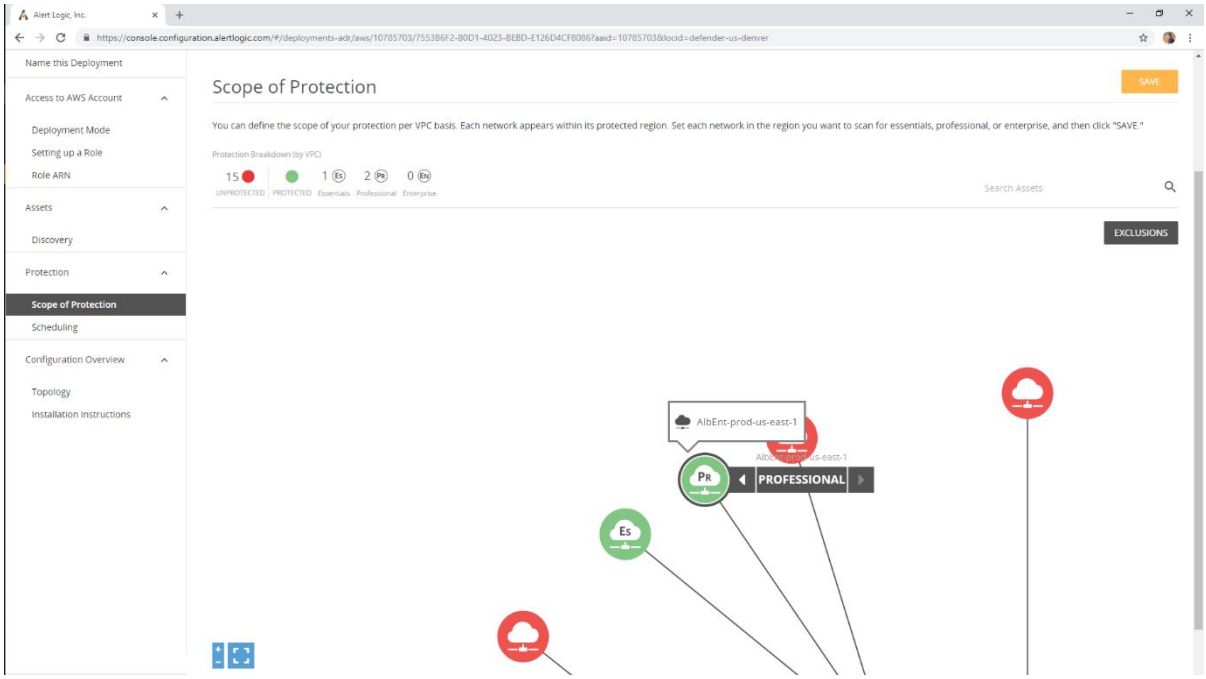
Alert Logic SIEMless Threat Management

Let's take a look at how Alert Logic approaches monitoring within AWS. In the Essential tier of our SIEMless Threat Management offerings, we use both active and passive cybersecurity tactics (network internal, external and PCI vulnerability scans, asset discovery, AWS CloudTrail collection), and for the Professional tier we add additional passive monitoring (NIDS, server log collection) to enable 24x7 monitoring by our SOC (security operations center). On the passive side, we use a role to collect Cloudtrail logs for security/asset discovery along with integration with GuardDuty and Security Hub. We use agents to collect host log data off the individual EC2 instances. Uniquely, we also use the agent to mirror network traffic from each individual EC2 instance. In the case of containers, we have a containerized agent that performs the same function, collecting log data and giving visibility into all container network traffic with Docker / Kubernetes metadata. This network traffic from agent-to-appliance is how we provide technology parity in hybrid deployments while taking advantage of unique characteristics of platforms such as AWS or Docker.

Operationally, you want to make sure that the agent is as low impact as possible, both in terms of resource utilization and deployment. The Alert Logic agent and container agent are both lightweight agents that are focused on offloading as much processing work to the appliances as possible. Today, that means that all network data is simply copied and sent to the appliance, and all syslog / file logs / Windows Event Log data is sent directly back to Alert Logic. We typically observe low single-digit percentage resource utilization on the underlying base host. In the near future, we will also be adding further host-based monitoring capabilities to the agent which will not add significant resource utilization, as correlation is offloaded to Alert Logic in the cloud.

Deploying SIEMless Threat Management

Deployment can be achieved in either an automated or manual mode. In the automated mode, you select which regions or VPC's you want to cover, and Alert Logic will automatically deploy appliances in the appropriate Availability Zones only when they are needed, and then scale them down when they are no longer necessary. In the screenshot below, you can see how different parts of your environment can be protected at different levels simply by toggling the mode as seen in the screenshot. Agents can be either baked into the image you are using or deployed using orchestration tools such as Chef, Puppet, or Kubernetes. These agents will then automatically configure themselves to communicate with the appropriate appliances, whether you choose to automate appliance deployment or not.



If you do not want Alert Logic automation to manage the deployment of appliances, you have the option to manually deploy the appliances. We will share the appliance AMI (application management interface) with you so that you can easily configure it where you would like. Even in the manual deployment mode, the appliance will still configure itself, and agents will still bind themselves to the correct appliance within the environment.

Simplify and Streamline Cybersecurity

When selecting security tooling, it's vital to balance your security needs against the effort of deployment. All too often, the difficulty of deployment results in security solutions not being fully deployed. In order to get deep visibility without a lot of operational impact on the host, on the network, and at the platform level, it's critical to ensure that configuration remains easy as possible.

To learn more about SIEMLess Threat Management, watch the webinar 'Why You No Longer Need a SIEM Tool'.

About the Author

10+ years' experience dedicated to IT security and compliance, with over 5 in Sales Engineering. Work with mid-market and enterprise customers, with a current concentration on developing channel partners. Focused on architecting technical solutions around physical and virtualized IDS / Log Management / Web Application Firewall Solutions, customer / partner training, and operational integration.

Backups like The Last Resort

The importance of backups within organization landscape.

By Pedro Tavares, Founder of CSIRT.UBI & Cyber Security Blog seguranca-informatica.pt

Today we live in an age where technology is part of everyday life for most people. ***Have you ever wondered if all the information on your smartphone and your personal computer was corrupted or lost?*** Your photos, contacts, important documents; with no chance of being recovered. Of course, this would be a very unpleasant situation in your life.

Looking at the day-to-day of an organization, the big picture is nothing different. If this situation would be complicated for a person, imagine what would happen if an organization lost all data. Sales information, customer and supplier data, contracts, sensitive files with large years of history, etc. Certainly, any digital catastrophe would do a great deal of damage to the organization, both reputational and related to the market position - the organization would probably close the doors.

Data Integrity

Internet of Things (IoT), Artificial Intelligence (AI), Big Data and social networks — it was not necessary to enumerates CRMs, or even to speak about databases. Some of these 'words' have leveraged the amount of information currently available in organizations. Digital data has thus become the new petroleum, and guarantee its integrity, confidentiality and availability is increasingly important.

Backups like The Last Resort

The main purpose of a backup is the replication, the copying of information for future restoration or consultation in case of loss, unauthorized alteration or damage to some type of file or digital system, and even until a natural or digital catastrophe.

The backup should preferably be performed on an external drive, and at different geographic location points, to prevent a type of damage from affecting different backups (which would be a huge problem).

Different devices for backups can be highlighted:

- External HD;
- Magnetic tapes (not in use);
- Local and isolated servers (standalone); and
- Cloud-based backup services (e.g., AWS S3).

Each option has its advantages and disadvantages. For example, an external HDD is more portable than most other solutions. For Cloud-based solutions, it does not expose the information in an online service that could potentially be exposed to cyber-attacks, and information subject to data breaches.

However it can also be damaged or misplaced more easily than a cloud-based solution. In addition, creating snapshots in a multi-device location may become less viable and time-consuming.

Organizations have for many years opted for the use of automated backup solutions on their own servers. Despite the high installation costs, this type of tool brings more security and privacy to those who do not want to transfer the structure to the Cloud. In addition, this type of backup allows for greater scalability and supports a large amount of data.

Cloud backup, on the other hand, has been notable in recent years for its low cost, high scalability and security. Today, companies in the industry can deliver services that use secure connections, encrypted data storage for a low value. With an internet connection, it is possible to hire a tool that can be accessed anywhere in the world for the configuration of a security backup routine.

Take the Sunday Afternoon to Think About the Subject

Cyber threats are constantly increasing. Technologies and software tend to become increasingly complex, with more lines of code (LOC), and with that the number of faults and potential vulnerabilities also tend to increase.

With this in mind, cybersecurity must be on the agenda of the meeting as a priority topic. There are no bulletproof systems. Note that the exploitation of a zero-day vulnerability could compromise an organization. If a solid backup security policy has not been established, some of the server configurations, software licenses and sensitive information may be corrupted and destroyed.

It's therefore essential to lay out all points of failure to prevent and avoid problems this nature. These problems can cause irreversible damage to market positioning and consumer confidence.

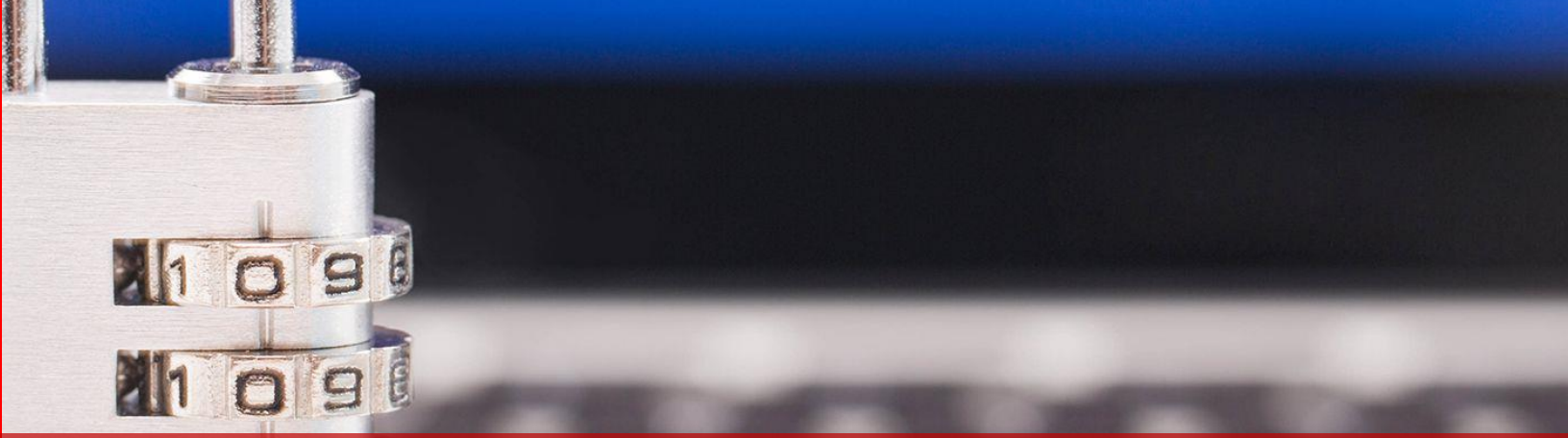
About the Author

Pedro Tavares is a cybersecurity professional and a founding member and Pentester of CSIRT.UBI and the founder of seguranca-informatica.pt. In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, hacking, cybersecurity, IoT and security in computer networks. He is also a Freelance Writer.

Segurança Informática blog: www.seguranca-informatica.pt

LinkedIn: https://www.linkedin.com/in/sirpedrotavares

Contact me: ptavares@seguranca-informatica.pt



Cutting Through the Hype—The Realistic Flaws of a Zero Trust Security Model

By Morey J. Haber, CTO, BeyondTrust

A zero-trust security model redefines the architecture of a trusted network inside a defined corporate perimeter. This is relevant today since technologies and processes like the cloud, DevOps, and IoT have either blurred, or completely dissolved, the idea of a traditional perimeter. But while zero trust has become a trendy catchword in IT here in the Middle East, in practice, it remains more of a theoretical concept as opposed to one that organizations can implement, for a couple of reasons.

Legacy internal applications

If your organization develops its own software for internal consumption, and the applications are more than a few years old, you may have technical debt. Loosely defined, technical debt refers to solutions based on older or obsolete technology that would not be used to develop new solutions today. Applications written in Cobol are an extreme example of technical debt.

Today, redesigning, recoding, and redeploying applications to replace technical debt can be costly and potentially disruptive. There needs to be a serious business need to undertake these types of initiatives. Adding security parameters to existing applications to make them zero trust-aware is not always feasible. Odds are your existing applications have no facilities today to accommodate a zero trust model.

Therefore, depending on how reliant you are on custom applications, this will dictate whether or not you can adopt zero trust to those processes, and potentially determine the effort and cost required. This is especially true in instances when applications are not microperimeter compatible, or lack Application Programming Interfaces (API) to support the required automation for a zero trust implementation.

Legacy Infrastructure

Legacy infrastructure and network devices are most certainly not zero trust-aware. They have no concept of least privilege or lateral movement, and they do not possess authentication models that dynamically allow for modifications based on contextual usage.

Any zero trust implementation requires a layered, or wrapper, approach to enable these systems. However, a layered approach entails wrapping the external access to the resource and rarely can interact with the system itself. This defeats the premise of zero trust. You cannot monitor the behavior within a non-compatible application. You can screen scrape, keystroke log, and monitor logs and network traffic to look for potentially malicious behavior, but your reaction is limited. You can only limit the external interaction of the legacy device to the user or other resources—but not the runtime itself.

This limits the coverage of zero trust, and based on the characteristics of legacy infrastructure, organizations may find that even monitoring network traffic is not feasible due to heavy encryption requirements, including emerging standards like TLS 1.3.

P2P Communication

If you think your organization does not use peer-to-peer (P2P) networking technology, you are probably unaware of the default settings in Windows 10.

Starting in 2015, Windows 10 enabled a P2P technology to share Windows Updates among peer systems to save internet bandwidth. While some organizations turn this off, others are not even aware it exists. This represents privileged lateral movement between systems that is fundamentally uncontrolled. While no vulnerabilities and exploits have materialized for this feature, it does present communications that violate the zero trust model. There should be no unauthorized lateral movement—even within a specified micro perimeter.

In addition, if you use mesh network technology, you will find that they operate completely counter to zero trust. They require P2P communications in order to operate, and the trust model is based strictly on keys or passwords with no dynamic models for authentication modifications.

Therefore, if you decide to embrace zero trust, you need to investigate if your organization has P2P or mesh network technologies, even for wireless networks. These present a huge stumbling block to embracing the access, segmentation, and microperimeter controls required for zero trust.

Digital Transformation

Even for organizations that are in a position to build a brand-new datacenter, implement a role-based access model, and embrace zero trust 100%, there is the challenge posed by digital transformation.

The digital transformation driven by Cloud, DevOps, IoT, and IIoT does not inherently support the zero trust model as it requires additional technology to segment and enforce the concept. For large deployments, this can be cost-prohibitive, and may even impact the ability for the solutions to interact correctly with multi user-access. If you doubt this, consider simply the storage requirements and license costs to log every event for dynamic access on all resources within the scope of the project.

While some may disagree that the Cloud does embrace segmentation and zero trust models, it all depends on how you use the Cloud. A straight migration of your raised floor to the cloud does not embrace zero trust. If you develop a new application in the cloud as a service, then it certainly can embrace zero trust.

However, just moving to the Cloud alone as a part of your digital transformation does not mean you inherently get the prescribed zero trust model benefits. And if you decide to embrace zero trust and bake it into your plan, your results may be limited for all the reasons discussed earlier in this article.

The zero trust model is not new. Regulatory standards like PCI have embraced the concepts, minus analytics and automation, for years. The basics make common sense, but without considering the existing technology within your stack, your strategic direction, and the technologies used for remote access and vulnerability management, it is just a theoretical approach used for architecting good cybersecurity hygiene from the ground up, not a pre-packaged solution that can be bought to retrofit over your existing systems.

Therefore, the only successful zero trust implementations that have gone from marketing to reality are ones that have baked zero trust in from day one. These are brand new end-to-end designs with minimal legacy interactions. Typically, this is not something everyone can do unless they are embarking on a brand-new initiative.

About the Author

With more than 20 years of IT industry experience and author of Privileged Attack Vectors, Mr. Haber joined BeyondTrust in 2012 as a part of the eEye Digital Security acquisition. He currently oversees BeyondTrust technology for both vulnerability and privileged access management solutions. In 2004, Mr. Haber joined eEye as the Director of Security Engineering and was responsible for strategic business discussions and vulnerability management architectures in Fortune 500 clients. Prior to eEye, he was a Development Manager for Computer Associates, Inc. (CA), responsible for new product beta cycles and named customer accounts. Mr. Haber began his career as a Reliability and Maintainability Engineer for a government contractor building flight and training simulators. He earned a Bachelors of Science in Electrical Engineering from the State University of New York at Stony Brook.

Enterprise Insider Threats on The Rise

New report finds 59 percent of organizations have experienced at least one insider attack in the last 12 months

By Rich Campagna, CMO, Bitglass

With news of hacking incidents, new strains of malware, and other alarming external cyberattacks, many organizations can overlook the importance of remediating insider threats. Comprised of both negligent and malicious employee behaviors, these threats pose a legitimate danger to enterprise security. To learn more about the state of insider threats and what organizations are doing to defend against them, Bitglass partnered with a leading cybersecurity community to survey IT professionals. The results, captured in the 2019 Insider Threat Report, revealed that insider attacks are on the rise. Unfortunately, they also showed that most organizations don't have the proper security controls in place to identify and defend against these harmful attacks which can stem from employees, partners, or other internal stakeholders.

In the survey, 73 percent of all respondents said that insider attacks have become more frequent over the past 12 months; 59 percent said that their organization has been victim to at least one over the same timeframe. These numbers are significantly higher since the last time Bitglass conducted this survey in 2017. While this is likely due to a multitude of factors, two key themes did seem to emerge from the research. The first is data moving off premises, and the second is the fact that companies often fail to secure their data in the growing number of devices and applications that access and store corporate information.

The rapid adoption of the cloud and bring your own device (BYOD) means that data is no longer kept safe behind on-premises firewalls and other traditional security tools. In fact, in separate studies, Bitglass found that 81 percent of organizations around the world now use cloud apps, and that 85 percent of organizations now enable BYOD. These numbers indicate that companies are embracing new technologies that offer numerous benefits; for example, greater cost savings, improved productivity, and more collaboration, as well as enhanced employee satisfaction and retention. However, this fundamental shift in where and how data is stored, used, and shared demands a different approach to security. Unfortunately, Bitglass' latest research suggests that many companies are failing to adapt accordingly.

The first issue uncovered in the report lies with the monitoring and detection of insider threats. 56 percent of organizations said that it is more difficult to detect insider threats after migrating to the cloud. Despite this, 41 percent claimed that their organizations don't monitor for abnormal user behavior across their

cloud footprints. Furthermore, only 12 percent of enterprises reported that they are able to detect insider threats stemming from any personal mobile device. While an additional 39 percent said that they can detect these threats if personal devices are used on premises or have agents installed, this is not as helpful as it may initially seem. BYOD means that data is frequently being accessed remotely – outside of the network perimeter. Additionally, employees tend to reject agents on their personal phones because they can invade their privacy and impair the functionality of their devices. In other words, the aforementioned 39 percent still need to take steps to secure personal endpoints from insider threats.

In addition to the above, many companies are failing to employ other tools and practices that are needed to stay safe. Alarmingly, only 50 percent of organizations are providing user training to combat insider threats. As many of these threats are caused purely by negligence, training employees on security best practices (such as password hygiene and how to spot phishing emails) has proven to be effective. Most employees want to help keep their company secure, but need to know how their actions fit into the equation. Another area in which organizations must improve is in the use of secondary authentication. While the tool is helpful for preventing malicious data access when users surrender their credentials, a mere 31 percent of organizations stated that they currently use it. In light of these issues, it is not surprising that 68 percent of organizations felt moderately to extremely vulnerable to insider threats.

Enterprises wishing to adapt to today's dynamic business landscape through the use of cloud, BYOD, and other innovative solutions must be able to detect, prevent, and respond to insider threats. By understanding modern risks and leveraging appropriate security solutions like cloud access security brokers (CASBs), the vast majority of insider threats can be reduced or even eliminated.

About the Author

Rich Campagna is the CMO of Bitglass. He joined as VP of products and has served in various roles at the company. Prior to joining Bitglass, Rich was senior director of product management at F5 Networks, responsible for access security. Rich gained valuable experience in product management and sales engineering at Juniper Networks and at Sprint before working at F5. Rich received an M.B.A from the UCLA Anderson School of Management and a B.S. in electrical engineering from Pennsylvania State University. Rich can be reached online through Bitglass' website: http://www.bitglass.com/

Your Security Teams are Destroying Critical Evidence

Why Stopping Siloed Attacks is No Longer Enough

By Erik Randall, Security Engineer, Exabeam

Gone are the days of smash-and-grab cyberattacks: Cybercrimes are now sophisticated sequences that take place over hours or days. Resolving the attack sequences requires SOC analysts to see the complete picture. But far too many security analysts responsible for triaging events lack the understanding and tools to give them proper situational awareness to the activities of modern attacks.

Seeing the Whole Attack Chain and Destroying the Evidence

With so many alerts to handle, Tier 1 SOC Analysts need to pick the most severe cases to deal with first and get to the others when they have time. These "triage specialists" must balance volume, judgement on severity, and like any position, performance metrics. Performance is often measured in ticket resolution rates and median time to response (MTTR), so there is pressure to resolve quickly.

Many SOCs provide their Tier 1 analysts with runbooks—a set of standard procedures for resolving common incidents. While theoretically prudent, runbooks can have a detrimental impact: while they often aid in resolving a particular alert, they can also end up destroying evidence that might be needed to investigate a more serious security incident.

Analysts typically take action against discrete Indicators of Compromise (IoCs) then close the ticket and move on. But an attacker is not done once the machine is infected with malware; that's just a foothold toward larger goals.

Think of a laptop infected with malware. A common SOC runbook procedure is to remove the threat by re-imaging the machine. Threat removed. MTTR low. But while the threat is gone, so too are all the artifacts that would have helped a Tier 2 or Tier 3 analyst find the source of the attack. *You might even go so far as to say the analyst is helping the attacker by deleting all the evidence for them!*

Uncovering a Compromised Insider

Imagine this scenario: An attacker wants to steal the source code for a new product from the leader in the market. They're going to compromise the machine of an engineer inside the company's network and use that as a jumping off point to search the network and find code repositories with product software.

Thanks to a new framework from MITRE called ATT&CK, we can realistically detail the techniques an attacker might use to pull it off.

First, the attacker sets up a watering hole attack, knowing that an engineer at the target organization is likely to visit the website of an upcoming user conference. Once the engineer visits the website (Drive-by Compromise), the malicious code on the webpage is triggered and executed by the browser of the engineer's machine. At this point, the attacker achieves code execution (User Execution) to gain a foothold on the targeted machine.

After this initial execution, the attacker then covers their tracks by deleting a portion of the malware on the system (File Deletion), in an attempt to avoid detection.

Now that the attacker controls the machine, they locate an SMB share that may contain the desired data (Discovery). As it turns out, the desired data requires privileged credentials, so the attacker escalates privileges to gain access to a user account with administrator credentials (Lateral Movement). Now the attacker can access the file share and copy over the sensitive data.

Next, the attacker will steal a token from a login script that was run with a privileged domain account (Privilege Escalation), gaining access to a server in the DMZ and the ability to move data out of the network. Now the data can be copied to the server and compressed in preparation for transfer over the internet. The attacker then connects from the server in the DMZ to an attacker-controlled web server. And just like that, they've stolen your new product source code.

In this scenario, many of these tactics and techniques would have at some point set off alarms in most SOCs. But while the alerts may get investigated, too often the response by lower-tier analysts ends up incomplete, and the attacker has already gained deeper access into the organization's network and systems. By the time an attacker reaches Lateral Movement, the trail often goes dark for SOC personnel, since it is very difficult to distinguish between activity driven by the real user of an account and an attacker using that account. And it is also this stage that the sensitive theft is taking place.

To ensure optimal protection, security teams must change their mindset to start looking at entire attack sequences instead of individual steps. SOC teams need to be able to compare a user's behavior to their normal patterns in order to understand if compromised credentials are being used by an attacker.

Using Behavior to Detect Complete Attack Chains

User and Entity Behavior Analytics (UEBA) allows security analysts to do just that. UEBA products take a thumbprint of what activities are normal for each user and compare that to activities the user performs in near real time. Coupling that with tactics and techniques known to be risky from ATT&CK, UEBA interfaces then highlights the activity as being both atypical and risky. The more of these tactics and techniques that an attacker uses, the higher the risk score within UEBA interfaces and the more this stands out to SOC analysts.

By tying together the behaviors identified as anomalous and risky with the techniques identified in the ATT&CK framework, responders can now trace the steps an attacker has used and predict where they may be heading next. Only once the attack chain is fully understood can the SOC analyst then take appropriate remediation steps to preserve evidence instead of re-imaging the system and possibly destroying key evidence needed to perform additional forensic examination of the compromised system.

Given the gravity of the compromises depicted here, every piece of evidence in this crime scene needs to be preserved for the duration of the investigation. Each incident needs to be seen as part of a bigger picture. Closing a ticket is not the same thing as solving a crime.

About the Author

Erik Randall is a Security Engineer at Exabeam. He is an information security leader with proven success implementing leading-edge technology solutions while balancing risk, business operations and innovations. Specialties include security service management, systems architecture, network design, and systems administration with extensive experience in engineering, manufacturing, services and financial industries.

Reflecting on April Patch Tuesday

Updates This Month from Microsoft, Adobe, Wireshark, Oracle and Opera

By Chris Goettl, Director of Product Management, Security, Ivanti

Ever wonder why there are so many updates in April? I figure it is fate giving me an overwhelming number of updates so I can abuse the old adage about April showers bringing May flowers, but what do April patches bring us in May? Hmm… it will come to me.

While I noodle over that, let's dig into the lineup for April because it is CRAZY!!!

We got updates from Microsoft, Adobe, Wireshark, Oracle (dropping on April 16), and Opera. We also have a boat-load of end-of-life notices, which raise a number of security concerns that are very timely to discuss, given the recent Arizona Tea ransomware attack that brought the company to a grinding halt.

Microsoft has released 15 updates resolving 74 unique CVEs this month. These updates affect the Windows OS, Internet Explorer and Edge browsers, Office, SharePoint and Exchange. Two of the vulnerabilities (CVE-2019-0803 and CVE-2019-0859) resolved in the Windows OS are being used in exploits in the wild. These are Win32k elevation-of-privilege vulnerabilities that could allow a locally authenticated attacker to run arbitrary code in kernel mode.

Adobe has released seven total updates resolving 43 unique CVEs. Adobe Reader, Acrobat, AIR, Flash, and Shockwave are the most concerning here. You can get updates for Reader, Acrobat, AIR, and Flash, but Shockwave has reached its end-of-life so no update is available for its seven critical vulnerabilities.

Immediate action: remove Shockwave from your environment! Its seven vulnerabilities are going to leave the majority of Shockwave installs exposed. You can bet an exploit is imminent there.

Wireshark released three updates resolving 10 CVEs. Wireshark is one of those overlooked IT tools that can pose a significant risk to your environment. Ensure it gets updated or removed where it is no longer needed.

Ivanti Priorities this month:

- Patch the Windows OS and browsers
- Patch Adobe Reader, Acrobat, AIR and Flash
- Remove Shockwave from your environment unless you have a continued support contract with Adobe to receive updates
- Patch Wireshark
- Investigate the Office, SharePoint, and Exchange updates and get them rolled out in a reasonable timeframe
- Review end-of-life software in your environment and have an action plan in place to eliminate or mitigate risks. I would suggest:
    - Remove it (best option)
    - Virtualize the workloads
    - Reduce access
    - Segregate from the rest of your environment
    - Limit or remove internet connectivity to those workloads

So if you caught my April Patch Tuesday Forecast on Help Net Security you have seen the nice long list of end-of-life products I went through. Add Shockwave to that list now. Also, if you have not caught up on the latest news we have a real-world example of how neglecting this issue can come back to bite you. Arizona Beverages was hit by a large-scale Ransomware attack that brought the company to its knees. The incident was attributed to outdated systems and systems with updates not yet applied as well as poorly configured backups. Take the time to review this list and look into other products in your environment. Obsolete software is a considerable risk to your environment and needs to be addressed even if removal is not the immediate answer. Have a plan in place to mitigate the risk if elimination is not possible.

Recent and upcoming end-of-life announcements:

- Windows 10 branch 1709 (for Pro licenses) – April 9, 2019
- Windows 10 branch 1607 - April 9, 2019
- XP Embedded POSReady 2009 - April 9, 2019
- Java 8 (last update was January 2019) – January 2019
- Adobe Shockwave - April 9, 2019
- Windows 7 - January 14, 2020
- Server 2008 - January 14, 2020
- Server 2008 R2 - January 14, 2020

About the Author

Chris Goettl, is director of product management, security, Ivanti. Chris is a strong industry voice with more than 10 years of experience in supporting, implementing, and training IT Admins on how to implement strong patching processes. He hosts a monthly Patch Tuesday webinar, blogs on vulnerability and related software security topics, and his commentary is often quoted as a security expert in the media.

Chris can be reached online at chris.goettl@ivanti.com, on Twitter @ChrisGoettl and at Ivanti's website: www.ivanti.com.

Phishing Awareness - The More They Know, the Less the Threat

By Matthew Goodwin

In this paper, I will be going over what phishing email attacks are and how end user training can help secure an organization against such attacks. In my organization, I am responsible for securing our network from threats and employee training plays a large part of that. I will go over some of the different things end users need to be aware of when interacting with emails to ensure they are not opening their organization up to an attack as well as discuss recent attacks which have made the news. I will also discuss some of the different employee training tools that may assist organizations with training their employees to spot and mitigate phishing email attacks.

Email is one of the most convenient forms of communication that is used for not only business communication but also for personal correspondence. Due to email's wide usage and ease of use, it is the perfect courier for outside entities to use to compromise an organization. The most common attack method, called Phishing, seeks to trick an individual into clicking a link or opening an attachment by appearing to come from a legitimate source such as a friend or trusted business. Phishing emails are usually sent from malicious sources out to millions of recipients in the hope that some will fall for the hoax and infect their machines or give out personal information. According to Phishing (2015), "Phishing is similar to using a net to catch fish; you do not know what you will catch, but the bigger the net, the more fish you will find." Links and attachments in phishing emails are usually designed to either harvest information or infect the recipient's computer and/or network. Once infected, the recipient's file may be encrypted, and they will be forced to pay to have their files unencrypted or their machine may begin sending out phishing emails attempting to infect other machines. In March of 2018, the city of Atlanta was crippled by a ransomware cyberattack that encrypted much of their network and demanded a ransom. Atlanta's law enforcement, court system, city hall, and multiple municipal departments were all taken

down for days while teams worked to rid their network of the infestation. The cost of the city's response to the cyberattack is estimated to be around $17 million. It is not known if this infestation was started by a phishing email, but phishing email have the capability to deploy ransomware and infect networks once ran by the recipient. Even though most organizations have spam filters which will catch and stop many malicious emails from reaching their employees, some email will always get through, which is where employee phishing training comes in.

When an organization's prevention systems fail to block a malicious email sender it is up to the recipient to catch that an email is malicious and deal with it accordingly. Your defenses don't depend on high-tech anti-hacking coding, as much as they do on your people knowing what to look for and reporting attacks (Anti-Phishing, n.d.). Phishing emails can be tricky by their nature, but there are some things employees can look for to help spot a phishing email. The "From" address of an email is often a quick way to tell if an email is from a legitimate source because many scammers use email addresses that are close to legitimate sender addresses but are slightly different. If recipients take a second and double-check these "From" addresses, they should be able to catch the fake address and prevent the phishing attempt. Phishing emails will also usually request urgent action from the recipient in the hope that they will act quickly without thinking about their actions. Employees should be trained to be very cautious of any email requesting immediate action and when in doubt staff should contact their IT department before taking any action. Since most phishing emails are sent out to millions, the scammer needs to format the email's text to be relevant to most of its recipients, which is why a generic greeting can be a big red flag for a phishing email. Another big red flag of a phishing email are incorrect hyperlink or website address. If an employee hovers over a link in an email and the link that appears is different, then this is a strong sign that the email could be malicious. When organization employees receive these tips and others from Phishing training they are less likely to fall for the phishing attempt. A study performed by Gordon, Wright, and Aiyagari (2019) found that among a sample of US health care institutions that sent phishing simulations, almost 1 in 7 simulated emails sent were clicked on by employees. Increasing campaigns were associated with decreased odds of clicking on a phishing email, suggesting a potential benefit of phishing simulation and awareness.

According to HIPAA Journal (2018), A survey conducted by a consultancy firm Censuswide revealed that one in five workers had not been given any security awareness training whatsoever, but even when training was provided, many office workers still engaged in unsafe practices such as clicking hyperlinks or opening email attachments in messages from unknown senders. This survey result helps emphasize that just providing a training is not enough, but that you need to provide the right training for your organization and your organization needs to enforce that training. Just like there is no one type of phishing attack, there is not just one type of phishing training or training vendor. There are multiple vendors available today that offer great phishing simulation and training for end users and I will briefly discuss three noteworthy platforms include SANS Security Awareness, PhishingBox, and KnowBe4. SANS, a company well known for its training courses, offers a well-rounded end user training course which includes animations, live action scenarios, hands on simulations, and interactive cyber-attack games. SANS tailors its trainings to a large audience by making it available in over 30 languages and delivering training videos with subtitles, voiceovers, and transcripts. PhishingBox advertises their phishing awareness training as an easy-to-use platform that is mobile friendly and has real-time reporting. PhishingBox offers several training courses ranging from general information security to more targeted phishing awareness training and allows the organization to create their own training. KnowBe4, a

recognized leader for security awareness training, provides an easy to use training website with a training library of 850+ instructional and interactive training items. KnowBe4 also offers features such as Industry Benchmarking which compares your organization with other companies in the same industry, Phish Alert Button that allows end users to report phishing attempts directly from outlook, and USB Drive and Vishing tests to help train end users on various attack surfaces. All three of these training vendors provide similar services that are all intended to help an organization's end user be better prepared for a phishing attack. It is important for an organization to view various training options and find the solution that works best for them.

My organization chose to implement KnowBe4 for our employee security training and we have been pleased with the results. When we first started with KnowBe4, they performed a baseline simulated phishing test on our environment which resulted in about 24% of our organization's employees clicking on the simulated malicious link. These results helped drive the development of testing and training programs for our organization. Our testing program with KnowBe4 is a monthly simulated phishing attack with double-random message delivery. The test is double-random because it pulls from the top reported phishing attacks each week and the email delivery is spread over the month throughout working hours, so every employee can receive a different phishing email at a different time. This random testing help simulate variety and prevents one employee from clicking and then warning others, which throws off any results. Our training program utilizes KnowBe4 for both mandatory yearly training and remedial training. Every August, a training is selected from KnowBe4's inventory and deployed to be completed by all of our employees. Our organization supports this training with a policy which states if an employee does not complete this training in a timely manner then they will loss all computer access until it is completed. We also have quarterly remedial training for employee that click on simulated phishing emails. If an employee clicks on a simulated link, then their account is added to a group. About every four months, a training is selected and any employee that is in the group is automatically assigned to the training and notified both their supervisor and them are notified via email. If the employee fails to complete their remedial training in a timely manner, then they will also loss computer access. Our organization has been running this testing and training program for about two years now and on average our percentage of phishing email clicks has fallen to about 4%. It is our hope that continued training, coupled with increased support from management, will help bring that percentage even lower.

Awareness and training can play a large part of keeping an organization secure from phishing attacks. There are many types of phishing attacks but if an end user is aware of what red flags to look for, then they are less likely to fall for them. With many different companies available that provide security training, an organization should be able to find one that meets their budget and their needs. Do you agree that training is an essential part of security? If you oversaw an organization, would you implement a training program for your employees?

Work Cited

Phishing. (2015). Retrieved March 31, 2019, from https://www.sans.org/security-awareness-training/ouch-newsletter/2015/phishing

*Anti-Phishing: The Importance of Phishing Awareness Training. (n.d.). Retrieved March 31, 2019, from https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/anti-phishing-the-importance-of-phishing-awareness-training/#gref

HIPAA Journal. (2018, December 17). Study Highlights Seriousness of Phishing Threat and Importance of Security Awareness Training. Retrieved March 31, 2019, from https://www.hipaajournal.com/study-phishing-security-awareness-training-employees/

*Gordon, W. J., Wright, A., & Aiyagari, R. (2019, March 08). Employee Susceptibility to Phishing Attacks at US Health Care Institutions. Retrieved March 31, 2019, from https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270

Douglas, T. (2018, October/November). What Can We Learn from Atlanta? Retrieved March 31, 2019, from https://www.govtech.com/security/What-Can-We-Learn-from-Atlanta.html

KnowBe4. (n.d.). Enterprise Security Awareness Training. Retrieved March 31, 2019, from https://www.knowbe4.com/products/enterprise-security-awareness-training/

Phishing Awareness Training. (n.d.). Retrieved March 31, 2019, from https://www.phishingbox.com/products-services/phishing-awareness-training

SANS™ Institute. (n.d.). EndUser Training. Retrieved March 31, 2019, from https://www.sans.org/security-awareness-training/products/end-user

About the Author

Matthew Goodwin is a Network Manager with the Carteret County Government. For the last several years he has overseen the County's network, infrastructure, and security needs.

On Security and Privacy, States Are Taking the Lead

By Andrea Little Limbago, Chief Social Scientist, Virtru

When Toyota announced the second data breach of the year, initial signs pointed to the group OceanLotus, a Vietnamese-linked state sponsored espionage group. The Marriott breach, and the almost 400,000 compromised customer records, has been linked to China. These incidents continue the steady drumbeat of new data breaches linked to nation-states, but we're also seeing a rise in other sources of data breaches. An unsecured database accidentally exposed two billion personal records, while Collection #1 and subsequent collections' combined for 3.5 billion user records posted on a hacking site. Together, these compromises highlight the proliferation of attackers, the growing size of data breaches, and the prominence of unsecured and accidental data exposures. However, despite this proliferation, the United States lacks a federal privacy regulation to incentivize better protection and security standards while also introducing accountability. Absent a federal privacy regulation, individual states are initiating their own data protection and privacy regulations to help combat these threats and shift corporate incentives.

Data protection and privacy legislation are not usually included in discussions of the latest cyber defenses and the threat landscape. However, they should be viewed as core components for augmenting deterrence by denial. While many of the new and existing authorities develop deterrence by punishment, much less focus has been devoted to explicitly shifting incentives to prioritize data protections. In fact,

'assume breach' has become the dominant defensive strategy. While this may reflect the modern reality, our national defensive posture will never improve if we aspire to such a low bar.

Understanding the necessity for thoughtful regulation to help shift incentives to encourage greater defenses and data protection, and absent a federal law, individual states have proposed or passed their own data privacy and security legislation. At a recent Senate hearing on a federal data privacy framework, the discussion highlighted the growing patchwork of regulations in the United States, including over 90 data protection and privacy proposals currently at state capitols. Similarly, last year Alabama and South Dakota became the final two states to enact data breach notification laws. There are now over 50 different data breach notification laws in the United States, with Puerto Rico, the U.S. Virgin Islands, Guam, and Washington, DC also passing their own laws. Each of these data breach notification laws has different requirements and penalties, and may be contradictory from state to state.

The most prominent piece of state privacy legislation is the California Consumer Privacy Act (CCPA), which will take effect in 2020. The CCPA focuses on unauthorized data access and intentionally targets both cyber attacks and third-party data disclosure violations. Individuals can hold organizations accountable for failing to protect their data, while organizations are required to implement "reasonable security measures" to protect their data. Accountability is core to any data protection framework as it provides the necessary incentives to drive organizational change in favor of security. Despite the range of cyber attacks and third-party data sharing, accountability has largely been absent in the United States.

Vermont has taken a different approach and passed a law focused on the data brokers themselves. As we saw with Equifax and the Office of Personnel Management breaches, organizations with significant amounts of personal data are ideal targets but may not prioritize implementing best security practices. Data brokers have largely remained off the radar but manage significant amounts of data. Vermont's data broker law requires data brokers to take appropriate security measures and penalizes them for failing to do, while also prohibiting the use of the data for criminal purposes. This is the first such law in the United States that holds significant data aggregators and sellers accountable for data security.

Legislation introduced in Massachusetts, Washington, Colorado and Washington, DC further reflects the current movement toward greater privacy and security in the absence of a federal framework. Largely driven by the ongoing data breaches as well as unauthorized data sharing, these laws explicitly aim to incentivize greater data protection as well as transform data sharing and storing practices, while also looking ahead to the future data challenges with biometrics, surveillance, and facial recognition. Left unprotected, these too will be a gold mine for bad actors.

Given the steady pace of security and privacy hearings on the Hill coupled with new state-level privacy laws, as well as foreign laws such as the European Union's General Data Protection Regulation, the likelihood for U.S. federal privacy regulation continues to grow. Until then, states are setting the bar and forcing the federal government to evaluate what core components should be included at a federal level.

This federal push will not be a silver bullet and requires thoughtful and deliberate input from the security community. If it includes accountability and enhanced security measures as core components, federal data privacy regulations may finally provide the impetus for organizations to prioritize security and limit the hemorrhaging of data that is the current status quo.

About the Author

Dr. Andrea Little Limbago is the Chief Social Scientist of Virtru, a data protection and privacy software company. She specializes in the intersection of technology, information security, and national security, and specifically focuses on the geopolitics of cybersecurity, global data protection and privacy trends, and usable security. Andrea is also the Program Director for the Emerging Technologies Program at the National Security Institute at George Mason. She previously was the Chief Social Scientist at Endgame, a cybersecurity software company. Prior to that, Andrea taught in academia and was a technical lead in the Department of Defense. Andrea earned a PhD in Political Science from the University of Colorado at Boulder. Andrea can be reached online on Twitter @limbagoa and at https://www.virtru.com/ .

Zero Trust Security

Security for the Cloud-Native Era

By Amir Sharif, Co-founder at Aporeto

Cybercrime on the Rise

Every day, hackers succeed at gaining access to the well-protected systems. Adversaries are more skilled and better funded than ever, and traditional security measures are ineffective. In 2018, cybercrime cost the global economy an estimated $600 billion – about 0.8 percent of global GDP. Security, previously an afterthought in the world of cloud-native applications, has come to the forefront with this barrage of data breaches that highlight critical flaws with legacy data center security systems.

These flaws? In a word (or two): IP addresses, and IP-based security. In the cloud-native era “location” is no longer bound to a single data center; using IP address as a proxy for identity in an attempt to secure applications becomes a fool's errand.

Castles and Moats

While most data centers are virtualized, they operate with the assumption that what is inside the firewall can be trusted, and what is outside cannot. This is also referred to as the “castle-and-moat” mentality, which focuses on the defense of the perimeters and turns a blind eye to anything already inside the castle walls (presuming they have previously been cleared for access). This highlights a key failing of firewalls and traditional perimeter security at large. If a malicious presence manages to gain access to the infrastructure, it can easily begin both north/south and lateral attacks and wreak havoc before its presence is even questioned.

Despite its present-day failings, this was an acceptable approach to security when applications were monolithic or had a classic three-tier architecture. With the dawn of the cloud-native era, however, applications have become disaggregated across public and private cloud, and using IP addresses to secure applications becomes risky business. Broad adoption of both mobile and cloud technology has begun to erase the data center perimeter. (One way to visualize this is as your handheld devices as

miniature bridges - an email can cross the defensive moat between the corporate IT infrastructure and your personal cloud in mere nanoseconds).

Zero Trust Fundamentals: Trust No-one

To secure a cloud-native application, we must embrace Zero Trust security and expand our thinking beyond legacy solutions to evolve with new application architectures. Application security must be thought of in terms of authentication and authorization: trust no-one, and authenticate, authorize and encrypt everything.

These are the key tenets of Zero Trust security.

Eliminate network trust

Segment network access

Gain visibility and analysis capabilities

Trust No-one

Zero Trust as a concept establishes a security paradigm based on the assumption that any system can be accessed and breached at any time, by anybody. You must trust no-one: even those already inside the network perimeter.

You can apply this to any structure - a cloud application, a data center, a bank vault, the aforementioned castle-and-moat, or your own home. Building security controls from a basis of Zero Trust allows you to keep data, property, confidential information (or even your family) safe.

Assigning Dynamic Workload Identity

Traditional approaches to security are two dimensional: based on IP address, and therefore, location. True application identity must be formed using a multi-dimensional trust profile. Consider approaching an application as you would a person, or a colleague: you automatically generate a dynamic trust profile based on their face, mannerisms, gait, height, voice, and other identifiers that – collectively – are unique to them. This same dynamic approach must be taken to confirming application-identity and must be assigned at a granular, workload level.

Legacy Security is failing

Micro services, containers and cloud are allowing enterprises to build and deploy applications with ever increasing speed. However as applications become distributed across public, private and hybrid clouds, it becomes increasingly difficult for security teams to maintain control and visibility into what is going on. Deployment speed is increasing; security is struggling to keep up.

Migrating to the cloud swiftly and securely requires a shift in mindset from static, perimeter-centric security towards a Zero Trust model. Deploying this model restores control to security teams by making security scalable, automated and infrastructure agnostic.

At a moment when it feels the quest to secure the enterprise is spiraling out of control, fear not. The concept of Zero Trust is increasingly gaining traction across the sector, providing promising new approaches for securing IT systems – a light at the end of the tunnel as the flame from the firewall diminishes, flickers and goes out – forever.

About the Author

Amir Sharif is Co-Founder of Aporeto. He has 20 years of experience in virtualization, networking technologies, and low-latency I/O. His experience includes running business development, product management and software development teams at Parallels, VMware, Topspin (Cisco), and Sun.

Amir can be reached via email at amir@aporeto.com, on Twitter at @amir_sharif or through Aporeto's website, www.aporeto.com.

Network Traffic Analysis (NTA)

By Timothy Liu, CTO & Co-Founder, Hillstone Networks

Network Traffic Analysis (NTA) was first created and defined by Gartner as an emerging category of security solutions that use network communications as the foundational data source for detecting and investigating security threats and anomalous or malicious behaviors within that network.

NTA was named one of the top 11 emerging technologies in 2017 by Gartner. As the technology is maturing, security vendors are delivering a variety of solutions that directly utilize NTA or integrate NTA as part of an overall threat protection solution platform.

On February 28 2019, Gartner published its first market guide for NTA. In this report, it has provided an overview of the NTA technology landscape, has set the market direction and analyzed corresponding products from leading vendors. This is the first and most critical guide on the NTA market since the category was first created a few years ago.

Here, we will first go over the key functionalities and elements of NTA technology. In the second part, we will discuss some major functionalities of the NTA platform from Hillstone Networks.

What is NTA?

NTA technology itself has been around for a while. It has been widely used in network monitoring and traffic analysis; it can help provide comprehensive visibility of the entire network to gain insights into network operations and performance, among other things.

As it turns out, today, cyber criminals, casual or professional hackers and other sponsored organizations are using more and more advanced techniques and tools to stage cyberattacks; these are more targeted, persistent and sophisticated attacks and their goals often involve stealing useful user credentials, critical

business data and other information for monetary purposes. Legacy threat attack detection and prevention mechanisms and technologies which are usually deployed at network perimeters using static, signature rules based mechanisms are becoming insufficient to fend off these sophisticated attacks.

With advancements in cloud computing, as well as data mining and analytical techniques driven by AI and machine learning, a wide range of new network security technologies are emerging that have proven to be more effective — in conjunction with other legacy security techniques — to detect, prevent and respond to more advanced threat attacks. One of them is NTA.

Instead of checking static pattern signatures and policy rules, NTA continuously monitors and collects network traffic and other packet data information. Over a period of time, it can form a baseline for traffic and use the baseline to represent normal traffic patterns and behaviors of applications and services inside the corporate network. More importantly, these also represent the normal behaviors of the users that are accessing these applications and services. In other words, network traffic is closely related to the user conduct that generates these traffic patterns.

Once the baselines are established, new traffic from the same traffic flows are checked against the baseline and network traffic is analyzed based on mathematical or machine learning algorithms. Consequently, abnormal traffic and application services patterns, which indicate the abnormal behavior of corresponding users, can be detected and comprehensive analysis can be presented visually to security analysts and admins. Proper actions can be taken to eliminate or mitigate any potential damages.

The Anatomy of NTA

A typical NTA platform usually consists of these key elements:

Traffic Collector

Different type of network traffic such as traffic logs and pcaps are collected, parsed, normalized and forwarded to the data storage module. Usually there are protocol decoding functionalities in the collector modules. Collectors can be physical appliances or software agents installed on the end user devices. Collectors are usually deployed in tapping mode to minimize impact to normal business operations.

Traffic Data Storage

Formalized traffic data are stored in one or multiple databases in either a centralized or distributed manner. Traffic logs or metadata can be queried and searched flexibly and efficiently. Typically, data is stored for a prolonged period of time which can be used for threat detection, threat hunting and forensic evidencing purposes.

Since the amount of traffic logs usually are very large, there are requirements for database capacities and query efficiencies. Modern technologies like Hadoop and Elasticsearch stacks are commonly used to store and retrieve traffic data in the distributed architecture. For NTA to be effective, it is crucial to collect traffic logs for the entire protected network over sufficient lengths of time. This is critical in traffic correlation analysis and also for comprehensive threat hunting capabilities.

Traffic Analysis Engine

These are the work horses of NTA. There are many analytical techniques that can be applied ranging from simple statistical analysis to much more complicated machine learning based algorithms. The goal is to identify the applications and services whose traffic patterns exceed the derivation thresholds from the established baselines.

Output Module

As the results of traffic analysis, logs and alerts are generated, they are presented visually in the user interface for security analysts and admins to take mitigation actions, such as pushing firewall policies, blocking suspicious hosts or performing traffic control associated with compromised hosts.

NTA technology is critical to cyber security. It provides an effective and powerful tool to gain insights of real time network and application traffic, especially east and west network traffic, which is often associated with lateral traffic movement and data exfiltration after an attacker breaches the corporate network. This is critical in detecting post-breach threats, as well as those unauthorized activities from inside the corporate network, whether done intentionally or unintentionally, by corporate employees.

Hillstone delivers on and helps you understand and act on network traffic analysis

In Gartner's NTA Market Guide, the Server Breach Detection System (sBDS) from Hillstone Networks was selected by Gartner as the leading product after comprehensive reviews.

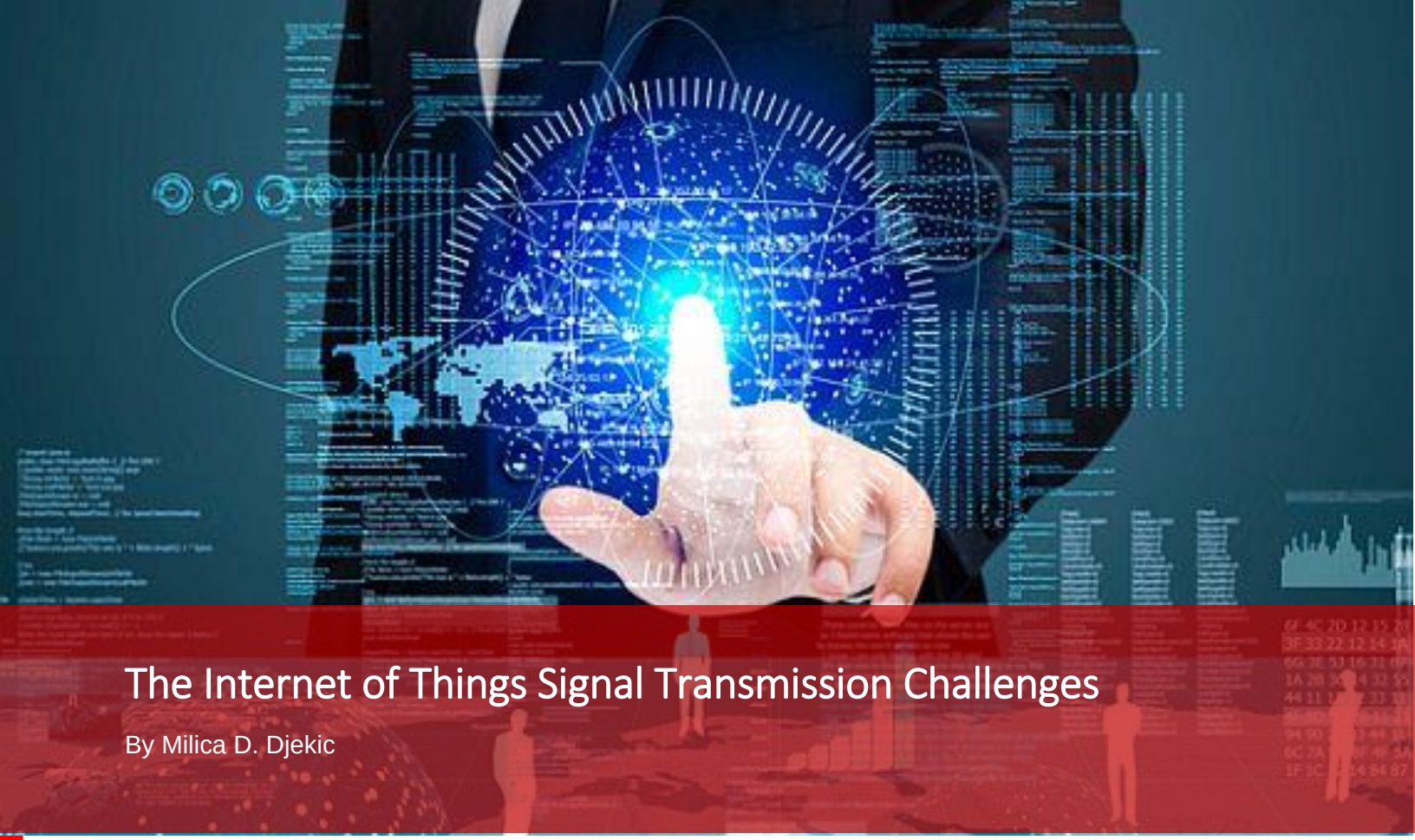
The sBDS platform integrates multiple threat detection engines such as Intrusion Prevention System (IPS) and antivirus. Without decrypting SSL/TLS traffic, layer 7 traffic metadata are collected and baselines are established during what is called the **learning mode**. Subsequently, real time traffic is continuously monitored and analyzed during what is called the **detection mode**. Using advanced mathematical algorithms to identify deviations from normal activity, any abnormal activities can be effectively detected and flagged. sBDS also integrates with Hillstone Next Generation Firewalls to add blocking capabilities.

In addition, Hillstone's NTA solution has self-adaptive capabilities. Any false positives or known exceptions such as holidays and vacations periods can be marked and applied to the future relearning and analysis either manually or automatically. The Hillstone NTA solution primarily targets the data center, with many dashboards focused on this use case. It can be deployed inside the corporate network as well as near protected server farms or host groups.

Hilstone's NTA solution is part of the full Hillstone Networks security and risk mitigation platform, delivering layered protection that allows enterprises to detect abnormal user and application behavior, thereby protecting enterprises from attacks, especially insider threats.

About the Author

Timothy Liu is a veteran of the technology and security industry for over 25 years. Mr. Liu is co-founder and CTO of Hillstone Networks, responsible for global marketing and sales. As CTO, he is also responsible for the company's product strategy and technology direction. Prior to founding Hillstone, Mr. Liu managed the development of VPN subsystems for ScreenOS at NetScreen Technologies, and Juniper Networks following its NetScreen acquisition. He has also been a co-architect of Juniper Universal Access Control. In the past, he has served key R&D positions at Intel, Silvan Networks, Enfashion and Convex Computer. Tim can be reached at our company website https://www.hillstonenet.com/



The Internet of Things Signal Transmission Challenges

By Milica D. Djekic

The Internet of Things (IoT) is a quite fast growing landscape and it's so important to understand why its safety and security matter. That technology would be vitally dependable on the internet connectivity, so if we lose a touch with the web – we would get something that is less usable at some level. It's so significant to get why we should take care about the entire IoT project's initiation which should include the intelligent definition of the cybersecurity requirements. For instance, try to imagine how it would work if your smart home, building or city appliances would cancel their functioning at the Christmas or New Year Eve when the majority of people on the North Hemisphere intend to enjoy the wonderful family moments. It's quite clear that some extreme weather conditions worldwide could paralyze the huge regions over the globe and those are something we should put under our control using the smallest amount of time to repair all the disaster consequences that occurred somewhere. The similar situation is with the critical infrastructure such as the electricity systems, so far, which could get the target of some devastating weather states or even skillfully planned hacker's attacks. As it's well-known, the IoT infrastructure would count about 50 billion devices so soon globally and that mass usage could recognize such a technology as the critical infrastructure for a reason its collapse could impact so many people on the planet. The internet signal is also critically important information carrier and as the IoT solutions vitally depend on the web connectivity – it's quite clear why we need to protect such a communications channel. Finally, the IoT is finding its place amongst the industry and manufacturing sectors, so the challenges of its safety and security are far more obvious.

The Source Spots of Internet Connectivity

The internet is a global network that would rely on a large number of servers, datacenters and providers serving to assure the entire infrastructure and provide the good communications channels to all end users. The IoT technology is something that would mainly be in hands of the web's consumers and if there is no internet connectivity at the endpoint the reason for so could be far more different. In some

cases, the web source spots such as the internet providers could get preoccupied with some flaws and unable to offer the good internet connectivity. Even in the less developed world – the web providers could serve thousands of clients and the majority of those end users could apply the IoT advancements at their homes or works. From such a perspective, it's quite obvious how inconvenient could be if someone's refrigerator with so delicious cake inside so could get disadvantaged over the summer season in case the IoT controller of that device got malfunctioned or if there is no the web signal with the smart heating system at someone's home or intelligent printer within some office which could reject to work as suggested. That's the quite unpleasant experience, right? The point is the internet providers should provide the reliable web service to their end users because of the quite dramatic impacts to the entire public and private sector in case of the web asset collapse. The fact is the internet source spots should use the cutting edge tools for their risk prevention, monitoring and incident response and it's highly recommended to apply the security operating centers as the part of your so critical internet infrastructure.

How to Manage the Web Signal All the Way Through

It's well-known that the hurricanes could damage the entire electricity infrastructure and leave millions of people without the electrical power. For such a reason, we see that asset as being the critical one. The equivalent situation is with the internet transmission lines. They can go through wires being below the ground or wirelessly being in the air. If anyone tries to do some kind of sabotage to such a system that would mean your server would work well, your device would not be infected anyhow – but you would not be capable to use your IoT gadgets. So many experts would agree that it's quite challenging to diagnose such damage, so that is some suggestion to the web professionals and such is to try to manage the risk of the entire grid discontinuity. We should always be aware that there are so many malicious actors who could get the sick idea to dig in front of someone's house or building in order to cut off the internet cables to such a neighborhood. They even may offer some sort of explanation that they are the workforce which does some repairing in that suburb. Anyhow, the teams of web providers' professionals should try to do the routine assessments of the landscape in order to assure the safe delivery of the internet signal.

What's going on at the Destination?

The final destination of the internet signal is the end user's device that is in the majority cases the part of some IoT network. In such a manner, we talk about the endpoint security or the methods how to prevent your computing infrastructure with the plenty of associated equipment to get distracted by the cyber criminals. Many researchers would mention that there are so powerful IoT search engines that could get applied in order to discover someone's IP address and put such a network under the risk. It's quite inconvenient experience if your IoT controller of, say, the heating system gets the malware for a reason your entire home or office could stay without the nice temperature and adequate humidity during the winter days. Also, if you lose your web connection due to some botnets and so intensive DDoS attacks – you will stay without your control signal to the entire consumer's destination.

Why is the Web Connection so Critical to the IoT Systems?

Either you are observing your web signal at its source, destination or the all way on – you should know that the internet connectivity is something that would provide the information exchange and functionality to the entire IoT network. Through this effort, we would mention how you can lose your web connectivity and let your IoT solutions getting so useless. This is not the critics to this fascinating technological boom, but rather the suggestion to the IoT designers to pay attention to some details that could mean a lot for

both – convenience and security of their products' users. As its name would indicate – the IoT would deal with the internet as its root and from such a point of view, it's quite transparent that the web signal would be the main data carrier with those solutions. In our opinion, the IoT is the good digital transformation of the existing technologies and at this stage, it means the progress – but we should get more confident about its suitability in terms of such safety and security. There are so many defense threats worldwide and those bad guys could try to take the opportunity to make our lives a bit harder and provoke the chaos amongst the good people of our human kind.

The Further Tips to the Next Generation Security Concepts

So many trickery experiences would show us that the IoT as the fast growing industry could get assumed as the critical infrastructure because of its so massive applications. For such a reason, it's important to think hard about its best practices in case of its safety and security, so we believe that the cyber, defense and intelligence communities would invest some time and effort in order to define some of the emerging concepts. In any case, it's so significant to mention that no internet would not only mean any communications through some period of time, but in the case of IoT gadgets – it could include much more dramatic impacts. Simply, the internet connectivity is something we use in order to make the entire systems work and at this point; we are quite concerned that the bad folks could try something to cause harm to many. Let's make the next chapters of our progress and prosperity being smarter and more secure ones!

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, 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 and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. 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). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

4 Signs Your Organization is a Good Cyber Attack Target, and What to Do about It

By Nathan Burke, CMO, Axonius

By now we're all well aware of the transformative technologies accelerating across the enterprise today. Trends like cloud, virtualization, BYOD, work-from-home, mobile devices, and IoT have completely transformed the way we work. However, in the process it removed the perimeter from the security picture, creating a massive, distributed attack surface.

As a result, organizations are under a continual onslaught of cyber-attacks leading to well-publicized data breaches. As their security defenses become more sophisticated, attackers will become increasingly opportunistic, looking to exploit lapses in IT environments.

This is especially true for organizations with complex IT environments. In 2019, companies that exhibit the following four characteristics are most likely prime targets for attackers:

1. **Proximity to Value:** Whether it's money or data, organizations that store valuable information will be targets. Banks are an obvious target since they are just one step away from actual dollars. However, organizations that store personal data (such as identity) to open a credit card or bank account need to be on guard.

2. **Centralized Data:** Companies that centrally store valuable information will be attractive targets to attackers. Taking the Marriott breach as an example, it was far easier for the attackers to obtain 500M records from the hotel's centralized reservation database than it would have been to go after individual franchise networks.

3. **Heavy Reliance on third-parties:** As we saw during the Target breach, the more organizations rely on third-parties, ecosystem providers and supply chain players, the higher risk of a breach that is outside of the organization's control.

4. **Cloud and Speed:** Companies that prioritize speed and convenience over adhering to security best practices to ensure all of their cloud instances are covered will be prime targets for costly data breaches.

So how can these types of organizations best shore up their security postures?

If you can identify with any of the above characteristics, the best course of action is to identify weaknesses and address the security fundamentals. Here are a few steps:

1. Understand What Assets You Have

You can only secure what you can see, and until you know which assets are in your environment, it's impossible to know whether those devices are satisfactorily secure. Understanding your inventory of laptops, desktops, servers, VMs, mobile devices, IoT devices, and cloud instances sounds simple, but organizations have a remarkably difficult time doing this. The first step should be establishing an ongoing device discovery, classification and inventory process to help you keep track.

2. Distinguish Between Managed and Unmanaged Assets

In any environment, assets can be split into two distinct categories: known/managed and unknown/unmanaged. Managed assets are known to security management systems (think endpoint agents and Active Directory.) Meanwhile, unmanaged devices may be known to the network, but do not have any security solutions installed so you aren't able to access its risk profile. Both types of devices are important but should be treated differently.

For example, a smart TV in a conference room is different from the CEO's laptop. While the Smart TV doesn't need an endpoint security solution or isn't part of a patch schedule, the laptop does. Creating a process to identify and take action based on asset classification is critical.

3. Address the Gaps in Security

Every organization has devices that are missing security solution coverage, whether it's iPhones without Mobile Device Management, or AWS instances not known to a VA scanner. Addressing these gaps in an ongoing basis is necessary, especially given the dynamic and elastic nature of these assets.

By following through on Steps 1 and 2, you'll be in a position to know all of the assets and their type in your environment, making it easier to identify where security holes are and how to best close those gaps.

4. Establish Ongoing User Access Auditing

For large organizations especially, keeping track of user permissions can be difficult. Are there users in your environment with local administrative access to all machines? Users with passwords that are not required or set to expire? Service accounts with keys to the kingdom? Even with strict access controls and regular policies, creating an ongoing auditing process is needed to ensure proper access rights.

5. Implement Security Policy Validation

The biggest question left to ask is this: How can I be sure that my security policies are being adhered to continuously? Whether you mandate that all assets must be scanned weekly, or you've determined that all Windows machines must have a specific endpoint agent, any security policy on paper is only as good as it is enforced and validated in reality.

Implementing a security policy validation process is the only way to make sure that nothing is being missed and that exceptions are being addressed and fixed instead of being exploited.

A Basic Framework

Putting solutions and technologies aside, cybersecurity is a discipline centered around understanding, addressing, and minimizing risk. Until you have a credible, comprehensive understanding of your environment and are able to understand where coverage gaps exist, you're at a disadvantage to those looking for a simple way in. With an understanding of all assets, gaps in security coverage, and the ability to see where the security policy is not being adhered to, organizations are in the best possible position to minimize their attack risk.

About the Author

Nathan Burke is the Chief Marketing Officer at Axonius. Passionate about bringing new technologies to market to solve real problems, he has held marketing leadership roles at Hexadite (acquired by Microsoft), Intralinks (acquired by Synchronoss), MineralTree, CloudLock (acquired by Cisco), and is a frequent speaker and contributing author on topics related to the intersection of collaboration and security. He lives on Cape Cod with his wife, daughter, and dogs, and enjoys watching the unfairly dominant New England Patriots. Nathan can be reached on Twitter at @nathanwburke, through LinkedIn, and on www.axonius.com.

Two Steps on – One Step Back

By Milica D. Djekic

Repeating is the mother of knowledge, the ancient Latin saying would suggest. Further, the Chinese proverb would tell – Practice leads to great skill or Practice makes perfect. Anyhow, in order to gain the skill you need to maintain some routine which would support you in becoming flawless with some responsibility. As the martial art practitioners would do the same spectrum of exercises again and again and get the black belt as the proof of their competency in that sport, we should apply the similar approach to the modern marketplace and its workforce. For instance, we believe that repeating the same routine again and again could increase your IQ for that area and make you obtain the brilliance in that field. There are so many people worldwide who got the good predispositions to some task and if we offer to those folks an opportunity to raise and grow developing their potential to full – we can expect the real champions in such sports. Your sport could be tennis, athletics, gymnastics or any other intellectual competitions. In other words, it's quite important to get that at the first glance; you need to deal with the talent pool which would provide you the access to young people getting the great learning curve to some business and at the second stage; you should understand that you need to work hard with those gifted people in order to produce the next generation of leaders. In this effort, we would use the word – sport – and in such a case; we would mean any kind of activities that seeks the players. The players could act independently or as the part of some team. Finally, any competition is nothing else, but the game where at least two sides would play in order to win such a match. Above all, we believe the similar way of thinking could get assumed in terms of security and its workforce.

The Rationale for Creating Security Training

Certainly there is the huge need for security education and training programs, but it's also necessary to make a selection amongst all the offerings that could get found on the marketplace. The decision makers who would approve the funds to some solution should care about the both – budgeting and purpose of the courses they intend to accept or reject. In so many cases, there is the big need for the training rationale that would provide you an opportunity to make the careful grading of offerings coming from your organization or the supporting contractors. Anyhow, it's so important to pay the great attention to some kind of training assessment forms that would help you to evaluate any proposal on. The modern security landscape is so flooded with so many different offerings, but even that amount of propositions is not sufficient to satisfy all the marketplace requirements. For instance, so many developing countries would miss the appropriate education and training courses in so many areas of business and that is especially the case with the small businesses which would undoubtedly suffer the huge lack of training to their workforce. Also, the security is an area that would need a lot of good practice and its decision makers should care about the practical impacts of once selected courses. In so many fast raising economies, the imperative in any field is the skill and if you offer the people a good mix of theory and practice – you would get in position to produce the next generation of the black belt masters in that sport. The point is whatever you do in your life or business – you need to exercise hard in order to maintain that level of skills on.

Could we memorize the entire Course?

The fact is if you spend 8 hours or several days on some seminar – you would get difficulties to memorize all those information on. It may appear as easy at the beginning to deal with the new concepts and topics, but as time goes on you would realize that only the few things would leave in your memory. The security itself is not only about the cyber defense, but there is the great role of physical protection amongst that field. So, the point is very simple! If you want to make your physical security workforce gets the skill in some martial art or the weaponry usage – you need to show the same and same routine again and again. In addition, there is the big deal of experience you need to gain in the practice in order to become the real master in your business. The similar situation is with the cyber defense! If you want to obtain the black belt for a cyberspace, you need to practice so hard in order to get the great skill, so far. Further, it's the matter of motivation how hard the people would want to make any progress in their business on and sometimes if you choose the good candidates to some security program you could use the assistance of your psychological team in order to estimate what drives those promising people. Finally, if you make the good mix of predisposition, motivation and practice – you would definitely produce the next generation leaders to your purposes.

Make Things Simple – Not Complicated

The experience would suggest that the people would mainly easily accept the simple concepts, while the complicated topics would only confuse them. It's so hard to accept something you cannot understand at the first glance and if there is no chance to take something new – you would get difficulties to lately apply so in the practice. In other words, you would get a lot of troubles to enforce the law or secure the cyberspace if you do not understand how those things work. The security is about the risk management! It sounds simple, right? Basically, it is – only if you find the right way to explain such a concept to your attendees in so understandable manner.

Always Take Care about Your Training Resources

The piece of paper can take all, some experts would assume. The fact is it's important to take notes about your activities and get the written clues about everything you do. In the modern world, so many knowledgeable people would suggest to document all you do in order to get a chance to lately repeat all you need to know about that subject. Also, it's significant to take the huge care about your security training resources either they are textual, audio or video by their character. The repeating is the mother of knowledge, so it's quite obvious why the need for the good resources is such a big.

Make Thinkers out of Your Defense Force

The people being the part of a defense force are at least so intelligent and anyone choosing such a career is the good learner. The most important thing with the security is to keep moving on and indeed, the security folks would commonly use their brain cells in order to tackle some satiation, concern or even challenge. In other words, make your security training getting inspiring and making the good guys think hard about their responsibilities. It's not that hard, is it?

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, 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 and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. 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). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

More than a Buzzword: Survey Reveals Cyber Threat Intelligence Trends

By Corin Imai, Senior Security Advisor, DomainTools

Cyber Threat Intelligence (CTI), the collection and analysis of information about current and potential cyber-attacks and attempts, has evolved significantly in recent years. The accumulation and research of cyber threat data across human insights, open source information and technical intelligence from cybersecurity tools, has reached mainstream adoption, according to according a 2019 Ponemon Report: The Value of Threat Intelligence from Anomali. Now viewed as a critical resource for enterprise security, CTI is widely relied upon to inform and develop proactive cybersecurity measures.

With new challenges emerging, improvements in CTI best practices have come at an opportune time. An ever-changing matrix across commoditized malware, nation-state actors, cyber cold warfare activities, and a broadening landscape of connected devices that need to be secured, is pulling cybersecurity teams in a myriad of directions. As cybersecurity technology has advanced, practitioners and experts have deepened their knowledge on how CTI is collected, shared and used. However, practitioners with relevant and appropriate expertise, leaves organizations lacking the resources needed to effectively stay ahead of threat actors. The shortage of skilled cybersecurity practitioners around the globe has never had more of an impact, according to research from (ISC)2 which discovered 63% of participating organizations are suffering through a shortage of IT staff dedicated to cybersecurity. Moreover, nearly 60% of respondents said their companies are at “moderate” or “extreme” risk of cybersecurity attacks as a result of the shortage.

Given these challenges, strategic use of CTI is critically important. Enterprises are beginning to recognize this and prioritize threat intelligence. The 2019 EMA Megatrends in Cybersecurity report found that threat intelligence is an important area of focus for security practitioners in the coming year. In the study, when asked “which of the following broad security initiatives are driving current priorities in your overall security program?,” respondents ranked improving threat intelligence among the highest in the ‘expanding’ bucket, at 57 percent, with only 8 percent of companies not prioritizing threat intelligence in some way.

To better understand trends around CTI best practices and how they have changed, the SANS Institute recently conducted its fifth consecutive Cyber Threat Intelligence Survey. The 2019 results revealed insights into CTI as a mechanism for cybersecurity detection, prevention and response, and how its use has evolved alongside the cybersecurity ecosystem.

Strategic Improvements

The survey results were clear that CTI is on an upward trajectory both in the number of organizations using it and the extent to which it is applied. Seventy two percent of respondents said they are utilizing

CTI in some way, which is an increase from SANS's 2018's findings (68 percent). Respondent organizations are leveraging it for threat detection, or response, or both. And an increasing variety of information – including indicators of compromise, threat behaviors, adversary tactics, attack surface identification, and strategic analysis of the adversary – is being used. Nearly one-third said they use threat behavior information and 41 percent use indicators of compromise.

In previous SANS surveys, security practitioners said they were focused primarily on raw threat data, but today, they have elevated their use of CTI to drive strategy. Sixty-four percent said strategic-level reports, with threat data relevant to their specific organization or industry, drive the most value and enable intelligence-driven threat hunting, another indication of increasing sophistication in CTI practices.

Redefining Best Practices

Areas of improvement also emerged in the survey. Collaboration and threat information sharing among peers and law enforcement are critical to unlocking the value of CTI, and 69 percent of survey respondents agreed that these practices improve the timeliness and relevance of threat information. While information -sharing programs were also recognized as valuable in a number of additional areas, only about half said they are collaborating in this way.

There is work to be done in better identifying and defining requirements as well. Only 30 percent of survey participants noted that they have their CTI requirements documented and 37 percent said their requirements are ad-hoc.

Enterprises looking to deepen the value of their threat intelligence programs have a range of opportunities to do so. These include improving collaboration, standardizing best practices, and taking the time to identify knowledge gaps. SANS recommends that industry practitioners continue to embrace new applications and methods for utilizing CTI. Leveraging it to roadmap user education programs was one suggestion given by survey respondents.

About the Author

Corin Imai is Senior Security Advisor for DomainTools. She began her career working on desktop virtualization, networking and cloud computing technologies before delving into security. Corin can be reached online at our company website https://www.domaintools.com/

The Privileged Account Security and the Internet of Things

By Milica D. Djekic

The Internet of Things (IoT) literarily flooded the marketplace and some statistics would suggest that so soon every single person in the world would deal with at least 10 such gadgets on average. In other words, we got so dependable to that product of the 4th industrial revolution and in case of the IoT infrastructure collapse – we could suffer the serious consequences globally. Would this put the IoT in the critical assets amongst some countries? In our opinion, if the US Department of Homeland Security could include the small businesses into the critical asset of the United States, the similar situation could happen with the IoT solutions. On the other hand, the small businesses are something that would impact over 50% of the nation's economy and if anything occurs with that infrastructure the consequences could get tremendous. Also, if your IoT gadgets stop working due to the lack of the internet signal – you should get that could be so inconvenient in case you deal with smart fridges, garage doors or even heating systems. The industry 4.0 would bring us the huge dependability on the web signal and if there is no internet – there would be no operability to the majority of the IoT smart home, office of industrial solutions. So, how this could get correlated with the privileged accounts and what are the privileged accounts and their security anyway? The privileged account is any well-controlled access to some critical infrastructure environment and such a system would rely on the well-developed procedures and policies that would recommend how to assure such an access. Well, the main question here would be if we could use the privileged account approach in case of the IoT technologies. The answer to this question is quite simple and it would indicate if we assume that the IoT private and business solutions are from the strategic importance to some nation – we could say they need the privileged accounts, indeed. The purpose of this insight is to make a closer look to the endeavors of the 4th technological revolution and suggest us how we could get more secure in such crazy surroundings.

What is the Privileged Account?

The privileged account is any access to the critical infrastructure that is well-maintained and controlled with the series of procedures, policies and login information. The hackers and some terrorist organizations would show the interest to make a breach to such an environment and in that manner; wound some nation or country. The privileged account users would often be the trusted individuals, but there is still the huge risk from the insider threats trying to approach the critical assets. Some studies

would show that it's so hard to access someone's privileged account if you do not count on someone being inside that organization and providing you the critical data. On the other hand, any critical infrastructure device could get vulnerable to cyber incidents and in that fashion; we could discuss a bit more the endpoint security challenges. In other words, it's crucially important to carefully manage the sensitive information for a reason if you leave your login details and security procedures as well as policies within some computing unit – the bad guys could get in possession of those information and use them to access the privileged accounts. Also, it's significant to mention that the privileged account is not necessarily the access to some could-based environment, but rather the approach to some computer, server or even datacenter. In other words, the privileged accounts could serve to protect some machine from being exposed to the malicious activities.

The Internet of Things as a Critical Infrastructure

So many people on the planet would apply the IoT devices through their everyday's lives and business activities and they would certainly get dependable on those solutions. For instance, there are so many IoT smart homes, buildings and even cities in the world and the functionality of those systems could get deeply correlated with the ability of those solutions to communicate using the web signal. The internet communications could get distinguished into three main spots and those are source, transition and destination ones. It's well-known that the critical assets would use the security operating centers in order to get safe or at least under the well-managed risk and the similar practice could get applied to the internet providers which would literarily feed the IoT solutions with their communications signal. For example, let's discuss the IoT smart heating system for a while! The IoT smart heating system would mainly deal with the computing device getting some software with so and that application would use the internet connectivity in order to exchange the information with the gateway asset. Any heating system would get the thermostat as the gadget that would control the functioning of the boiler that would pump the water to the radiators. In addition, the IoT smart device with its application on would send the web signal to the router and the router would talk to thermostat in order to make it obtains the desired temperature and the additional conditions in that place. If there is no internet connectivity – there would not be any operability to that system, so far. This could get so serious during the winter months because the hackers and even terrorists could disable your internet connection attacking your web provider and leaving you without the heating at, say, your Christmas Eve. This could get the challenge to so many IoT manufactures which would not take into account the security of their products and which would offer the quite unreliable solutions on the marketplace. In other words, we do not want to criticize anyone because the IoT is so fast growing landscape and so many small economies worldwide would see their chance to progress making and selling the IoT solutions. That's the quite convenient way to make a profit on, but do not be that selfish to put on the risk so many people over the globe.

How to Secure Your Critical Asset?

The best practice would suggest that one of the ways to protect your critical asset is to use the privileged accounts. Even if you cope with those accounts – you should always care about their safety and security. It's quite clear that if we include the IoT into the critical infrastructure – you would need to think hard about some alternative options how to make those solutions being so functional even without the internet connectivity. It would appear that in such a case we need to go a step back for a reason our web network is not that safe at all. Also, we would recommend to protect your internet providers and, in some manner, guarantee the security of your signal delivery. We live in the historically quite turbulent period for the entire human kind, so that's why it matters to think about your and everyone's security.

The Best Practice being applied to the IoT

The IoT technologies would undoubtedly need some kind of the best practices being applied to them. The first thought in that sense would be that we need the better security to all. The insecurity of the IoT advancement could cause the dramatic impacts to many people globally. We are fully aware that the industry 4.0 would bring the huge transformation of the existing technologies and in such a case we hope that the industry leaders would closely collaborate with the security community offering the opportunity to the technological consumers to get a peaceful nap while they use their emerging improvements. Maybe the privileged accounts and their security are something that could make us being more secure, but also there are a plenty of technological options that should get put into the consideration, so far.

The Future Comments

Resolving any engineering task could get the big challenge to any technical team and being so innovative and creating such a historical boom with the emerging technology is the big deal to the civilization's progress and prosperity. Unfortunately, we live in the era of so many social and economic challenges and in so many cases the security of many people could get threatened. Above all, do not make the new technologies turn against you, but make them being your good friend that would always support you. It's not that hard, you would agree?

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, 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 and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. 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). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

It's All About The Logs

Looking into Your Past Will Secure Your Network's Future

By Gary Brown, Principal Consultant/CISO, Mosaic451

We see it repeatedly. The newly installed CISO or CIO installs the latest blinky-box in "the quadrant." As they discuss all the great features and how it's going to help protect their network, it's discovered that while the device will get MOST of the logs, but there are still areas that aren't logging. Plus, nothing in the back end network getting aggregated and processed either.

A better investment of time and resources would be to get the entire network logging to a centralized log aggregator before organizations spend cash on the trendy blinky-box. Without a complete picture of your network, you get partial information, which can be misleading. Many CISOs understand this when it's presented, but surprisingly many don't understand the importance of proper logging.

Complete and accurate logs are the keystone of any effective information security program. Almost every aspect of infosec touches logs at some point. If you can't query the activity of every device on your network, dedicate yourself to getting that fixed - quickly. Don't waste money on a SIEM or a honeypot or anything else before you've addressed this Infosec 101 prerequisite first.

Many network admins don't seem to care if their backend machines get broken into, they care about production. Most companies with this approach do not have truly separate networks. They have VPN connections, bastion firewalls, or other protections that allow them to restrict access, but inevitably their production users live eat and breathe on the backend as well. They usually get their emails, do time cards, file expenses, and so on, all on the same machine that their VPN connections are made from or their bastion host passwords are typed from. If malware is on that machine grabbing credentials and the security analysts are blind to that, then they very well might not notice anything amiss on the production side. There won't be failed logins to alert on as the attacker will have the credentials. Don't fall into that trap. Monitoring your backend is as critical as your production network. You are only as strong as your weakest link, and logging is how you identify your vulnerable spots.

If you are pretty sure you've got your devices all ready to log to an aggregator, make sure all your other ducks are in a row.

- Wherever possible, send all logs to a centralized log aggregator – make it the known sense of truth. If you can, try to have your logs on a dedicated resource. That is to say, don't use your SIEM as a log aggregator, rather send all logs to the aggregator and have them forward to the SIEM (and whatever other resources you need logs from).

- Ensure everything is logging. Applications, operating systems, and network/appliance traffic. Log successes as well as failures. Be careful not to over log though. I've seen ambitious logging projects collapse miserably because they simply became overwhelmed with amounts of data they had not projected for. By throttling back from verbose logging to a more targeted approach they were able to get back on track.

- Ensure all sensitive logs are encrypted in transmission. If an attacker can sit on the wire and read your logs, they will be able to pick your bones clean.

- Be sure to spec your log storage devices (and budgets) properly – and plan for expansion. Logs can be large, even with little activity. Anyone who has ever sat watching a Wireshark capture on a Windows network will tell you that operating system is extremely chatty. It's surprising how much disk space you can chew up at a fast clip. Don't size your log storage for current consumption, but also for projected growth.

- At a minimum grab authentication events, security related events, device errors, database or file actions, and other critical pieces of information required to grab a minimal picture of what is happening on all machines.

- Pick a log format and stick with it. If you can, try to have all logs recorded in a common format. This makes parsing and searching much easier for all concerned.

- Make sure your logs are redundant, backed up, and recoverable. By this I mean:

    - make sure your logs are able to fail over to another system if your main aggregator fails
    - make sure you make frequent backups, with copies being stored off site
    - make sure you can recover your logs; finding out you can't during a legal discovery process isn't a place you want to find yourself in

- Pick a strategy that will best suit your needs. How frequently do you need to access logs, and how far back are your average searches going? Your budget and operational requirements will drive your decision making process.

- Ensure all devices are syncing their time to the same common source. Timestamp disparities are an analyst's nightmare, and render logs as potentially useless for investigative or legal use.

- IT/networking teams can very often be helpful in selling costs to the management, or even sharing budget, as effective logs are also very effective troubleshooting tools. When something breaks, it usually shows up in the logs pretty quickly. Wherever possible, make logging a shared vision between teams.

A well designed and properly implemented logging strategy is the best way to equip your team to effectively detect and investigate suspicious activity, as well as to provide audit capabilities. In this increasingly hostile world, why wouldn't you want to give them – and yourself - a head start?

About the Author

Gary Brown is Principal Consultant/CISO at Mosaic451. Mosaic451 is a managed cyber security service provider (MSSP) and consultancy with specific expertise in building, operating and defending some of the most highly-secure networks in North America

Gary can be reached online at gary.brown@mosaic451.com and at our company website http://www.mosaic451.com/

86% of Cybersecurity Professionals Expect to Move In 2019, There's One Way to Fight Against It.

A people first approach to security is critical for success but it seems challenging and sometimes daunting.

By Karl Sharman, Vice-President, BeecherMadden

Human error is the number one cause of breaches or incidents according to Willis Towers Watson (almost 2/3's of breaches). Some of these will be error, but some will be rogue employees or ex-employees. Our research at BeecherMadden found, that in 2019, 86% of cyber professionals are open to moving organizations. Losing security staff creates a business risk, as do disgruntled or disengaged employees. So how can you mitigate this key security risk?

A people first approach to security is critical for success but it seems challenging and sometimes daunting, especially when considered against the two statistics above. A potential solution is for the CISO to appoint a Chief of Staff. The Chief of Staff can focus on the people issues, without needing to have the technical expertise often found in cybersecurity teams.

When speaking about security staff departing, one of the most expensive of those is the CISO. Industry research suggests that the average CISO tenure is only a maximum of 48 months, with many packing their bags even sooner according to CSO. Bringing in a solid Chief of Staff to remove some of the day-to-day grind could help CISOs focus on the higher-level parts of the job, maintain a more favorable work-life balance, and possibly extend the 18-24 months into more longevity and company loyalty.

This person can drive cyber awareness training, internal education, hiring and retention strategies and bridge that gap across many business units in complex environments. Although this comes at a cost to the business, hiring and education can be far more detrimental to the bottom line as well as damaging market reputation. Furthermore, their exposure to the team will further provide insight into areas for development or preventable issues around staffing, risk or costs to the business.

Salaries have significantly grown in the last year and there is more competition in the market to recruit talented individuals – companies have to create the right environment with a security first approach to appeal to candidates on the market. The Chief of Staff position will provide this in abundance. Retention is a serious issue; Cyber Security Ventures have repeatedly stated about the lack of candidates compared to the amount of open vacancies in the next few years. This means that companies need to take more responsibility in taking care of their staff in such a demanding and ruthless market.

Education for the security team is another aspect that companies are overlooking. It is important not only for the individual, but also for the company itself. Continuous improvement is the only way to deal with the evolving threat both internally and externally. Cyber Awareness is an added benefit to this especially across the wider units of the business as many companies lack understanding of security awareness among end-users, which can lead to more security vulnerabilities (ISC)[2].

Finally, the Chief of Staff can be a spokesperson for cybersecurity within the business internally and externally to further drive market reputation for candidates, customers and clients. They will be different to a Human Resource or PR specialist as they will be specialized and knowledgeable on the market and have deep insights to share at conferences, meetings and interviews.

The Chief of Staff is an important role within government and many firms have turned to this model to support staff better for the long-term future of the company. However, cybersecurity needs this more than ever to compete and stand out in a competitive marketplace.

About the Author

Karl Sharman is a Cyber Security specialist recruiter & talent advisor leading the US operations for BeecherMadden. After graduating from University, he was a lead recruiter of talent for football clubs including Crystal Palace, AFC Wimbledon & Southampton FC. In his time, he produced and supported over £1 million worth of talent for football clubs before moving into Cyber Security in 2017. In the cyber security industry, Karl has become a contributor, writer and a podcast host alongside his full-time recruitment focus. Karl can be reached online at karl.sharman@beechermadden.com, on LinkedIn and at our company website http://www.beechermadden.com

Empower your Kid with Cybersecurity

Train Your Lil-champ to be a Cyber Warrior

By Devin Smith, Marketing Director, ReviewsDir

We, as parents always want the best for our kids; we want them to learn everything - right from crawling to driving - at the right time in the right manner. Its 2019, today's kids are more interested in being tech-savvy than to be an athlete; though gadgets are not that bad, the internet is also not just about p***, even growing up immersed in social media is not that threatening, if used appropriately. But we can't ignore the growing vulnerabilities attached to it.

Kids are independence-seekers, naive, innocent, curious, fearful of being punished, easily influenced, in nature; these are the reasons they are way easier targets for both offline and online threat artists.

Saving a kid from a pick-pocket or bullies at a high school is easier, but what about those invisible culprits sitting everywhere in cyberspace, finding ways to blackmail, harras, bully, fraud, and whatnot to trap the young minds.

"The gap between Generation Y with X making it harder for parents to keep up with the tech. changes that are affecting their lil champs."

We chauffeur our kids to school, to the playground, worry about their grades, try to serve them in the most perfect manner, but unfortunately, don't take their online privacy and security seriously; who will take this responsibility? Do you know, computer viruses, identity theft, ransomware, cyberbullying and many other threats are affecting children every day?

Let's take a look into a kid's exposure to the so-called world of internet.

You're Kid and the Internet - An Inside out!

A study back in 2015, revealed that teens spend nearly nine hours using social media, while kids between 8 and 12 spend an average of six hours per day; what about yours? Find it out, not only hours but his/her online practices.

When your child is online, normal safeguards and security tips are not enough! You may think your kid is playing a game, researching a paper, or just typing a homework, so, how could he/she be harmed?

You are right to an extent, but what if, while playing a game, the child unknowingly click a malicious notification - reflecting a mesmerizing edition of their favorite game- or unintentionally delete your important file? There could more "what ifs," the worst is when your child doesn't realize what has happened and don't share with you because of being punished.

Get to know them ASAP!

Is Your Kid at Risk While Online? These Figures might be of Help

If you think, malware, spyware, and other cyber-attacks are adult-only, then you are wrong; anyone with a high level of trust and limited knowledge is hackers' best target. The propensity of threats increases when kids and teens are active in chat rooms, video streaming, social-media surfing, and online gaming.

To play our part in the manner expected, we should know the internet consumption practices of our young minds; thanks to iamcybersafe.org for conducting a comprehensive internet usage survey among kids of grade 4-8.
Let's see what the survey holds;

- 31% of kids download adult music.
- 21% watched adult programs.
- 29% of kids use the internet inappropriately (something their parents won't approve.)
- 6% shopped online with a credit card without their parents' consent.
- 2% searched for the adult content.
- 62% clicked to adult site after a search.
- 53% access the internet other than homework every day
- 31% lied about age to stream restricted content; isn't a status offense?

The same study has also revealed that 40% of kids chatted to strangers online; let me brief how much information they have shared already.

- 53% of them revealed their contact details.
- 11% met a stranger personally.
- 15% tried to meet.
- 6% shared their address.
- 21% spoke on phone.
- 30% texted a stranger.

Does anyone want their kids to share any piece of information or even talk to strangers online?
Nobody wants any such thing to happen with their kids; it's our duty to provide a safer and secure future to our kids, keeping them away from increasing risks and threats.
There are so many threats lurking for kids in cyberspace, right from bullying to ransomware, but the most credit goes to identity theft.
Just imagine, what if your kid is in foreclosure on a property in another state.

Your Kid's Online Identity Holds his/her Future - So, Don't Risk it!

Why I am saying this, you will understand with the results of a study "CHILD IDENTITY THEFT" conducted by Research Power; it was conducted back in 2011, but still relatable.

- 10.2% or 4,311 of the children in the report had their Social Security number used by others – it is 51 times higher than the rate for adults.
- The largest fraud of $725,000 was against a 16-year-old girl.
- The youngest victim was just five months old; 826 were between the ages of 6 to 10, 303 were under the age of five, 1212 were between the ages of 11 to 14, while 1849 were between 15 to 18 years of age.

This is not enough, even your kid's identity can also be used to sell and purchase homes and automobiles, open credit card accounts, obtain a driver's license, and for secure Employment.

You must be thinking how could an unused social security number be beneficial to hackers? Find the reasons below; you will be surprised!

What Happened with Unused Social Security Numbers?

Unused Social Security numbers are more valuable than one can think of, thieves' pair them with any name and birth date; making it useful for illegal immigration and other organized crimes.

A child's identity is blank with the least discoverability; since the child doesn't use it for an extended time and even parents also take it lightly, that's why it becomes an easy target.

What happened then? This destroys a child's ability to win loans approval, acquiring a phone, obtaining a job or else.
Anyways, kids need to be protected! But, how? That's what I will tell you, don't worry about that!

Hey Parents! Understand These Top Cybersecurity Concerns

For better understanding, I am dividing the measures in four different aspects, have a look.

Messaging, Where Hackers Wait for Their Targets

All the social media sites have direct message features that letting our kids to connect with friends, family, and strangers. Cybercriminals use such platforms, placing links that redirect to malicious downloads and phishing sites.
These are some signs that you can teach your kid to be aware of;

- Messages with unusual misspellings, typos, and/or oddly punctuated.
- Messages asking for personal information like credit card password or pin, SSNs, etc; legitimate social media sites never ask such things through direct message.
- Messages claiming your account will be blocked unless a specific action will be taken.
- Mismatched links, to check, keep the over a link with; make sure the bar address matches the destination.

You can also visit the sites like scam-detector and teach your lil champs some common ways how cybercriminals spread viruses via direct messaging.

Video Games - If it's Online, It's Dangerous

Can you spot a kid who doesn't love video games? You can't; thanks to games for letting our lil warriors to share their experiences with others; there you will find a social component (chat or direct messaging). Although this practice encourages game-build imaginations and relationships but also helping hackers to find their potential targets; don't forget, there are 22 apps that are malware-loaded.
Playing games don't infect systems; it's only when our multi-taskers leave one game open and land on another.
Teach your kids to avoid such practices of hackers;

- Chat links or Pop-up ads - they often lure with avatars, skins, free coins, and even upgrades; once clicked, it leads to download an executable file. When you open, the malware program infects and steal data that could be your credit information.
- Fake login pop-ups, asking username and password to continue; sometimes it could be "under maintenance" requests - a social engineering ploy to lock and steal kid's profile.
- Fake ads, asking them to click for freebies; hackers use botnets to run a fraudulent ad scheme - more clicks, more money for hackers.

To avoid phishing scams while playing video games online, you need to empower kids with these tricks.

- Set the chat “friends only” options.
- Help your child to learn “no free lunches” lesson.
- Keep reminding hackers’ common tricks to them on and off.

Anonymous Sharing - An Easy yet Disastrous Practice

Anonymous sharing is what teens and tweens love the most; thanks to apps like Snapchat, Instagram, and others, allowing image posting and temporarily messages, but sadly, nothing on the internet is temporary, everything remains there in the cloud.

Cyberbullies take screenshots and use as a weapon against our young minds;
Although anonymous sharing reflects a healthy and open expression of freedom, but also make oversharing easier.

Before letting your child use such apps, discuss what information is suitable enough to share with the world and make them wary of messages with links or attachments; teach your kids to use the internet smartly.

Streaming Sites - Kid’s loved it!

Again, streaming sites like Netflix, YouTube, and others don’t bring viruses along, but yes, their comment section can host; don’t click any link randomly in the chats.

Teach your kids the problem areas: how video ads look like, the comments section, and where descriptions of links are inserted; you can also turn the comment section off.

Kids learning is not sufficient, we parents also need to play our part; only then we can protect our kids from Cyber thieves and data suckers.

Let’s practice together!

Role of Parents in Securing Kids Online Presence

- Enable YouTube Restricted mode to filter out inappropriate content.
- Encourage your kids, to use the YouTube Kids App, so that the content remained under control.

- Opt Parental Controls for all your kids' devices and apps; let them or help them set their Facebook privacy "Friends Only" and block certain content to restrict their streamings.
- Be engaged - Be it playing games, researching a topic, or creating a family newsletter, try to get involved with everything he/she does.
- Set-up two-factor authentication - It is an extra layer to protect from hijacking.
- Partition the system into accounts - Restrict their accessibility and privileges; this way you can keep an eye on whatever he/she is doing on the internet.
- Is your kid's computer in an open area? If not, then do it; keeping the system in a high-traffic area help you monitor his/her activities.
- Get the security toolkit ready - Installing a comprehensive software like antivirus, Firewall, VPN, and others, can solve many of the problems that I have mentioned earlier. These tools will keep malicious actors and activities away from your kid's online world.

Is Your Kid Online? If YES, then Control his/her Digital Moves

Cybersecurity is something that we don't actually bother until a disaster happens; so, now it's all in your hand - whether to wait for a disaster and react or be proactive.

Our responsibility towards our kids are not restricted to necessities and luxuries, we have to make them understand the importance of their online presence and the growing vulnerabilities.

Before wishing the kids a healthy and wealthy future, I want to pat on the back of all the parents out there for being conscious about their kids' internet safety. But mommies and daddies, only concerned never works, practical actions need to be taken; as the future of our kids is at stake.

About the Author

Devin Smith is the Marketing Director of the ReviewsDir. He is a tech-mech by profession, and also passionate into finding variant indulgence of the Tech World. He has studied marketing and now turning his exposure into the experience; when you find him playing soccer, it must be his spare hours. Devin Smith can be reached online at (devinsmith.fw@gmail.com) and at our company website https://www.allbestvpn.com/

Standardizing Security: Mitigating IoT Cyber Risks

(Part II of an II Part Series)

By Daniel Jetton, Vice President of Cyber Services, OBXtek
And
Carter Simmons, Deputy Program Manager, OBXtek

Introduction

In the first part of this discussion, we demonstrated the need for standardized security for devices within the Internet of Things (IoT) because the proliferation of these devices has gotten ahead of security, not only due to the vulnerabilities they may have, but the sheer ubiquity of this phenomena and the unknown amount of personal data that may be at risk. While the government has taken some action in the form of the *DHS Cybersecurity Strategy* and legislation like the *Cyber Shield Act of 2017*, a tried and true process must be adopted. We are moving forward on these things to some degree but need a defined standard.

The Risk Management Framework

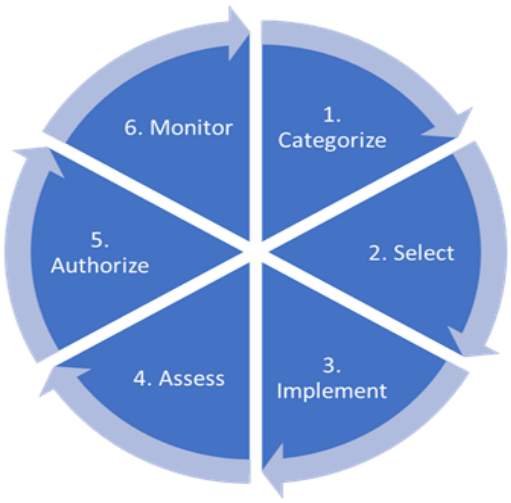
In February the National Institute of Standards and Technology (NIST) published the draft *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, also referred to as *NISTIR 8200*, to provide government and public entities information on developing and using cybersecurity standards in IoT systems, components and services. It is an artifact derived from the Internet of Things (IoT) Task Group, established in April 2017 by the Interagency International Cybersecurity Standardization Working Group (IICS WG) established in December 2015 to coordinate on major issues in international cybersecurity standardization. Specifically, it describes IoT and representative applications of IoT; reviews core areas of cybersecurity with relevant standards; details IoT cybersecurity risks, threats and objectives; analyzes current cybersecurity standards for IoT and; provides mapping of IoT cybersecurity standards to core areas of cybersecurity. NISTIR 8200 states that

"Standards-based cybersecurity risk management will continue to be a major factor in the trustworthiness of IoT applications and devices." IoT is unique and will require tailoring existing standards as well as creating new standards to address the wide array of IoT devices. Without these standards it would be nearly impossible to harden IoT devices across the board and across various sectors, while maintaining their functionality (NIST, 2018 Internet). In addition, the report states, "… the adoption of IoT brings cybersecurity risks that pose a significant threat to the nation."

In September 2018, NIST release a draft of their internal report (NISTIR) 8222 Internet of Things (IoT) Trust Concerns. In it, they break down 17 trust concerns that impact the security of IoT devices and services and is derived from their SP 800-183 ("Networks of Things"). They identify actions for mitigation and push additional areas for further exploration and study. As of the publication date of this article, the current draft has been withdrawn from the web, "to synchronize with other pending documents on this topic, and to ensure time for stakeholders to review and comment." NIST adds that, "Once the draft document has been re-posted, the comment period will be extended" (NIST, 2018 Interagency).

To expand upon this, we feel a NIST Risk Management Framework (RMF) approach may be used to secure IoT devices. The RMF is a common information security framework used by the federal government to improve information security and risk management processes. Simply stated, the RMF provides a review of an information system's security against established baselines. Identified risks are either fixed, mitigated, or deemed acceptable, in accordance with their usage. Once the system has gone through the testing phase of the RMF, the security and risk level of the system is vetted to the owner of the system. The designated "owner" may then accept the risk and grant the system an Authorization to Operate (ATO) on their network. The six-step process, involves 1) categorization of information systems based on impact due to loss of Confidentiality, Integrity, and Availability (CIA), 2) selection of security controls in accordance with a baseline and categorization results, 3) implementation of NIST security controls, 4) assessment of security controls addressing objectives and methods verifying compliance, schedule and procedures/validation and assessment with remediation as necessary, 5) authorization of information systems results in submittal and review of the package to the System Owner (SO) who will accept any residual risk and 6) monitoring of security controls to detect changes, their impact and updating of documentation to reflect current status. The cycle is typically three years before reassessment, unless other continuous monitoring strategies are in place.

Figure 1. The NIST RMF Process



Applying RMF to IoT

To effectively apply the RMF to IoT applications and devices, security categorization data types listed in NIST Special Publication 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories) would need to be updated for IoT and an A&A effort would need to occur with IoT developers. These are not the only things that would need to be tailored to apply RMF to IoT, but they are major factors. To properly categorize the IoT devices, new data types will need to be developed based on the type of data a system or device stores, processes, or transports. Once all the related data types have been selected, the IoT developer will be able to determine the CIA of their product. Based on CIA, the IoT developer can secure their product using a minimum-security baseline of security controls. The developer could conduct a "Type Authorization" on its products to establish a security hardening standard and ensure it is implemented with their respective applications and devices. This would force IoT manufacturers and developers to manufacture their components with security built in, meaning when an IoT device goes to market it will have already been hardened to a minimum set of security controls and configurations. As most of the world lacks security expertise, the average person would not be aware of or know how to better secure their IoT devices with best practices. Incorporating security-based configurations as default configurations within IoT devices would be a significant first step to securing the IoT environments.

Another Possible Solution (Plan B)

Underwriters Laboratories (UL) has worked in the public interest since 1894 providing safe living and working environments in 46 countries. Most people recognize that the UL symbol on a product certifies it as having passed their rigorous test and review process for safety, quality, and performance (Underwriters Labs, n.d.). Over the years UL has established standards for myriad devices including electric lamps, heating and cooling equipment, appliances, smoke detectors and power cords (Internet Archive Wayback Machine, 2002). Similar to the way UL works, another independent organization could be formed to certify security standards for IoT devices. The organization can be governmental or an offshoot of a non-profit. A non-profit organization may be the solution to developing new standards and administering/grading/certifying products similar to the way the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) stepped up to fill a void by creating standards for health care facilities. For example, the "IoT Accreditors (IoTA) Group" (let's call it) could be the one-stop shop for companies to secure their IoT gear before introducing it to the public. Any device with the IoTA™ logo would have gone through the rigorous testing and inspection process developed by the IoTA Group and accepted as

the de facto security standard similar to guidance from the Cyber Shield Act of 2017 about voluntary certification and labeling of IoT products.

A Fly in the Ointment

Whether we use a government agency like NIST, with established standards, or a non-profit organization like Underwriters Laboratories, who can develop their own standards for certification, one issue remains. The problem with certifying devices, in this day and age, is that the devices change. UL listed lightbulbs and power cords aren't typically upgraded, augmented or altered in any way. Alternatively, today's IoT products facilitate upgrades, updates, and modifications. While we may be heading in a positive direction with IoT security standards, alterations from upgrades, updates, modifications or added applications remain a major security certification issue. These alterations change the security configuration of a device, possibly voiding any prior certification and making the device vulnerable. Downloaded upgrades, updates, modifications and added applications means that the products that were once approved as safe are no longer the original secure product. The three-year NIST RMF cycle keeps government systems secure in continuity through continual review of any changes by the assigned engineers. Unless an IoT device is "set and forget" hardware that never requires alterations of any kind (unlikely in this day and age), they will need to be reviewed and re-certified when configuration changes are made. IoT security necessitates that: 1) IoT devices must be continuously monitored for changes to their risk status, 2) only pre-approved upgrades, updates, modifications and applications, in accordance with security certifiers, are allowed on the device and/or 3) IoT devices, once certified, are hardened to prevent any changes (i.e. set and forget/secure and endure). Any unapproved upgrades, updates, modifications or applications void the certification/security.

The configuration change vulnerability forces us to focus on the continuous monitoring phase of the RMF which addresses continued security to address configuration changes. Re-certifying security is considerably easier in a controlled environment where an organization can readily track changes and adjust devices and systems ad hoc. This is a lot harder when dealing with the public at large. There is no magic pill to keep devices secure/certified, but we offer a few ideas for contemplation. Perhaps IoT devices, once upgraded, updated or modified could be re-examined by running something similar to the virus scans we do on our personal computers. These scans would be device specific and provided by the manufacturer free of charge. The IoT devices could connect to a laptop to run diagnostics/scans in the same way your car can be connected to a diagnostic computer to run tests. After a scan, the results would show current vulnerabilities and offer downloads to fix those shortcomings. Simply put, every time a device's configuration changes (e.g. a downloaded update), a re-scan would once again certify the device as secure. Tesla vehicles receive "over-the-air" software updates that introduce new features and functionalities. There is no reason this same process can't be used for IoT security.

Without a solution that allows consumers to conveniently and cheaply secure a device, vulnerabilities will abound, and security will suffer. Certifications will mean nothing. Even making the process easy won't

necessarily ensure security. 14% of cell phone users admit to never updating their software and 28% do not lock their smartphone (Anderson and Olmstead, 2017).

Conclusion

The government, especially NIST, has taken strides to identify and mitigate IoT security concerns, but is yet to be seen how effective the DHS Cybersecurity Strategy, the Cyber Shield Act of 2017, NISTIR 8200 and 8222 are at this point. The NIST RMF, already a standard for systems security in the government, could be introduced as a proven process for securing IoT. Alternatively, non-profit organizations like Underwriters Laboratories and JCAHO have a definitive history of providing needed services to users by establish their own accepted standards for safety. Whether the government or an independent organization take the reins, it will be necessary to adopt security standards and mandate their use in establishing a base-level of security to protect consumers and secure IoT devices. While we have options for developing those standards and processes, the problem of keeping those devices secure in perpetuity in lieu of updates, upgrades and modifications will remain the primary challenge.

References

Anderson, M. and Olmstead, K. (2017). Many smartphone owners don't take steps to secure their devices. Retrieved from http://www.pewresearch.org/fact-tank/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/

Internet Archive Wayback Machine. (2002). Underwriters Labs3**.** UL's Standards for Safety Standards Catalog. Retrieved from

https://web.archive.org/web/20021105130017/http://ulstandardsinfonet.ul.com/catalog/stdscatframe.html

NIST (2018). Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT). Retrieved from

https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf

NIST (2018). Internet of Things (IoT) Trust Concerns: NIST Releases Draft NISTIR 8222 for Comment. Retrieved from https://www.nist.gov/news-events/news/2018/09/internet-things-iot-trust-concerns-nist-releases-draft-nistir-8222-commentUnderwriters Labs. (n.d) Our Mission: Working for a Safer World. Retrieved from https://www.ul.com/aboutul/our-mission/

About the Authors

Dan Jetton is the Vice President of Cyber Services for OBXtek. He is responsible for leading and defining cyber strategy while ensuring security, defense and risk mitigation for his clients. OBXtek's accomplished teams have an established reputation for consistently and efficiently achieving goals for its portfolio of federal government customers. Dan Jetton, MBA, MS, MA is a CISSP, CAP and PMP with 20 plus years of military service. He can be reached online at https://www.linkedin.com/in/danieljetton/ and at the OBXtek website http://www.obxtek.com/. You can follow him on Twitter @CyberPhalanx for cybersecurity news.

Carter Simmons, MS, CAP serves as deputy project manager on OBXtek's State Department Bureau of Consular Affairs and Office of Consular Systems and Technologies' Information Systems Security Support (ISSS) team on which he offers expertise in the risk management framework (RMF). In addition to his certification as a CAP (Certified Authorization Professional), he holds a master's degree in Cybersecurity from the University of Maryland University College.

Why Cyber Defense in the Power Industry is so Unique

By Gowri Rajappan, Director of Technology and Cybersecurity at Doble Engineering Company

Every organization connected to the internet is at risk of being the victim of a cyberattack. In fact, most organizations face multiple attacks per day with varying levels of sophistication. Electric power companies are more vulnerable than most. While most organizations have their networks in just a few locations, making them easier to defend, power company networks are sprawling, with potential access points everywhere.

While the adoption of new technology in the industry has done wonders for the efficiency and reliability of assets, it has also significantly increased the opportunity for hackers to gain access to the network. Nearly every piece of equipment in a utility's infrastructure contains a sensor that communicates performance data to the network. Many of these sensors represent-a point of vulnerability that could be exploited by a would-be hacker.

Speaking to Utility Dive in May of 2018, Bill Lawrence, director of the North American Electric Reliability Corporation's Electricity Information Sharing and Analysis Center said that, "In theory, a grid with more distributed resources can increase the potential attack surface for adversaries because the capacity of distributed generation, including renewables, has grown exponentially over the last decade."

This creates a different level of expectation when it comes to cybersecurity. Given the vast attack surface, it is not possible to successfully thwart every attack. It is important to have effective detection systems that can identify threats quickly, and rapid response plans to isolate and mitigate the detected threats before they can cause any damage.

While the management teams of most organizations would hold a fairly confident stance that their security systems could hold up to any outside attack, power and utilities have a very different perspective. A recent report issued by consulting firm KPMG highlighted that 48 percent of power and utility CEOs think that being the victim of a cybersecurity attack is inevitable.

According to KPMG's Global Sector Head of Energy and Natural Resources, Regina Mayor, "Technology-driven opportunities in the power and utilities sector have also opened the door for significant risks and cyber threats, which feature highly on CEOs' and board agendas."

Where is the security focus?

Keeping operations running and ensuring the safe and continuous flow of power has always been at the top of the agenda for power and utility companies. However, the escalation of cyber threats and attacks have caused company boards and C-level leadership to reprioritize some of their efforts.

In the recent years, the rise of nation state-based adversaries, motivated by the ability to shut down the operation and cut the flow of power, has driven much of the conversation. An emerging issue for power and utility companies these days is protecting customer data. Meeting customer expectations around data security is a priority as this directly impacts business performance and company value. For a distributed utility network with multiple access points, both are challenging without the right approach.

In KPMG's report, the firm highlights the role security plays in operations today, stating, "CEOs understand the importance of protecting customer data but emphasize the need to better meet customer expectations. Nearly two-thirds of all CEOs in the survey said that protecting customer data is critical to enabling growth in their future customer base."

How are they adjusting?

The good news is that power and utility companies have recognized the need for increased vigilance across the grid and are investing heavily in these areas. Cybersecurity specialists are among the most in-demand positions for power and utility companies.

With a well-earned reputation as technology laggards, the utility industry is giving a much greater effort to modernize more quickly and keep pace with the technological developments of other industries.

To address the issue of cybersecurity in any sort of meaningful way, utility companies need to adopt a big picture view and assess which assets need to be protected, where they are in the network, how the workforce should interact with those assets, and more. They then need to design a holistic solution that coordinates across silos to secure these assets. Industrial security today isn't insular. It's not homegrown. It's collaborative and intentional.

With every new opportunity comes a new threat. The electric grid is more robust and stable than ever before, but emerging cyber threats have made life more complicated for those charged with the safe delivery of this critical resource.

Being vigilant and making a commitment to cyber defenses and technology will allow power and utility companies to keep pace with adversaries and increase their ability to thwart attacks on their unique and vital infrastructure.

About the Author

Gowri Rajappan is the Director of Technology and Cybersecurity at Doble Engineering Company. He graduated with a doctorate in Electrical Engineering from Northwestern University in 2001, and has since spent over 15 years as a technology entrepreneur with extensive expertise in product development. For more information, reach out to Gowri at doble@corporateink.com or at our company website

https://www.doble.com/.

Data Sniffing is Threatening Your Personal IoT. Here's a Workaround

By William J. Tomlinson, Ph.D., Senior Member of the Technical Staff at Draper

The human body is becoming a node in the Internet of Things, and that may be creating more of a security threat than most people imagine. The problem goes beyond hackable passwords. Scientists say wearable technologies that rely on over-the-air data sharing could be giving away more personal data than previously suspected.

In the security field, we call it malicious eavesdropping, and it's a potential problem for more people as they adopt wearable devices. From body worn sensors to actively controlling smartphones via touch inputs, humans continuously communicate large amounts of personal data with the outside world.

The technology already exists for such eavesdropping. An attacker can simply make use of readily available methods, like an open source data sniffer, to steal unauthorized data by detecting the signals broadcasted wirelessly from commercial and wearable medical devices.

The capture of personal data isn't new. Recent news reports describe a breach that occurred when a fitness tracker worn by soldiers in training revealed location patterns of security forces working out at military bases in remote locations. Wearables ranging from smartwatches to Google Glass have been data sniffed as well.

To address this challenge, engineers from several organizations, including Draper, developed a new kind of secure transmission channel that uses the human body as a waveguide. The system leverages an intra-body communication (IBC) technique called galvanic coupling (GC), which is the coupling of low-level electric currents inside the human body, enabling wireless signal transmission through any region of the body to a receiver (via contact), such as a smartphone.

Our method of IBC can propagate information on and below the skin surface, into inner tissue layers with higher levels of conductivity. In our prototype, galvanic coupling offers moderate transmission distances and lower data rate compared to other methods but can safely operate with relatively high limits within the

human body. Its true advantages are low attenuation and full confinement of signals inside the human body, offering more security and interference-free communication.

Most importantly, we found that our prototype drastically reduced over-the-air leakage and adversarial detection of signals, making the transmission of biometric data impervious to sniffing attacks while still maintaining transmit power levels deemed safe for human operation. Ultimately, GC-signals are confined within the body and cannot be intercepted unless the user is in direct contact with the medium.

A key attribute of the system is its capability to secure data transmission for biological signals that have potential use for biometric authentication systems. Specifically, our prototype consists of a microcontroller unit (MCU) with supporting analog front-end hardware for signal modulation and detection. The transmitter MCU is configured to transmit with a biometric signature unique to the individual (in our scenario, the electrocardiogram signal). Other signatures might include, but are not limited to, electromyogram signals (EMAG), bio-impedance and galvanic skin response (electrodermal activity).

The adoption of biophysical signals, to either supplement or act as a stand-alone solution, as opposed to current antiquated authentication systems, lies at the cutting edge of biometric research for medical and commercial applications.

In the commercial space, there are wearable authenticators designed to work with other devices (desktop computers, doors, et al.) and perform authentication based on proximity to the locked device. Think of a fitness device or other wearable band that employs a biological signal as a biometric. Once a user is authenticated, the system will use wireless channels, such as Bluetooth Low Energy and NFC, to pair with devices running the supported application.

Wearables are also being developed that use a person's behavior for authentication. Whether it's something like a fingerprint scanner, a heartbeat sensor or an accelerometer measuring your gait, biometrics attempts to measure aspects of what you are, and those can be used for authentication. Devices in the fitness category can do this sort of measurement and are already gaining popularity. Combining biometrics with existing authentication factors can result in a very secure system that is nearly impossible to fool.

Recently, the use of alternative IBC solutions has been employed to perform similar operations. However, as we have demonstrated within our work, those signals are still susceptible to outside and environmental influence.

We describe our new biometric authentication system in a paper titled "Secure On-skin Biometric Signal Transmission using Galvanic Coupling." Our team, which includes engineers from Draper, Federal University of Parana and Northeastern University, presented our system at IEEE INFOCOM 2019 in Paris, France.

Funding for development of this technology was provided by a U.S. National Science Foundation under Grant No. CNS-1740907.

About the Author

William J. Tomlinson, Ph.D., is a Senior Member of the Technical Staff at Draper. He works in the radio frequency and communications systems group at Draper, and his primary interests are centered around developing hardware and software systems for wireless communication, spanning into applications such as Intra-Body Communication/Networks, Software Defined Radios, Wireless Energy Harvesting, Structural Health Monitoring and the Internet of Things. William Tomlinson can be reached online at https://www.linkedin.com/in/wjtomlin/ and at our company website http://www.draper.com/

The Role of Security Appliances in SD-WAN Adoption

By Brendan Patterson, Vice President of Product Management at WatchGuard Technologies

SD-WAN is one of the hottest networking technologies, and as we head into 2019 its growth is only expected to continue. As a matter of fact, IDC predicts the SD-WAN infrastructure will reach $4.5 billion by 2022. With more and more organizations relying on cloud applications to run day-to-day operations (such as Salesforce, JIRA, Confluence, Office 365, etc.), IT departments are under pressure to deliver high-quality, reliable links across the network. SD-WAN enables organizations to do this by curtailing expensive MPLS solutions, moving traffic to public internet lines, and often using secure VPN solutions to communicate between sites. This dramatically reduces transport costs, and in many cases increases performance. Network links without assured or guaranteed service can now be used to deliver business class services, including Voice over IP and video applications.

But as this market blossoms, what type of SD-WAN solution should companies be looking for and how could they impact a businesses' overall security? As with any emerging technology, there's no shortage of new vendors making bold claims, and every vendor's definition of the technology varies in order to match what they can deliver. That's why it's crucial for businesses to truly understand what SD-WAN is and what it isn't before embarking on a new deployment. And, in many cases, firewall appliances actually provide SD-WAN services now.

The ABCs of SD-WAN

When considering SD-WAN solutions, there are some key criteria every buyer should look for. The first is the use of software to manage connections over different link or connection types – MPLS, cable modem, DSL, 4G and links from different ISPs. Every SD-WAN service should offer dynamic path selection between these different links based on predefined policies set to align with business priorities. They should test circuit performance in real time, measuring packet loss, latency, and jitter to determine

if the line meets the acceptable level of quality for its application traffic. Second, you need traffic management for applications. For example, being able to guarantee 10 Mbps for all Salesforce traffic.

Third, when internet connections are used, businesses need to ensure that all data is private and none of the traffic can be viewed by third parties. This requires secure VPN capabilities for site-to-site tunnels with full IKEv2 level encryption or TLS level transport. And finally, "Zero-touch" deployment options allow SD-WAN appliances to be delivered to remote locations, and configured automatically by simply powering on and connecting to the internet. This ease of deployment aspect is critical, as technical staff and network engineers are scarce, and businesses need to quickly deploy cloud solutions as they roll out new hybrid WAN architectures to distributed sites.

(Note: SD-WAN is typically delivered by placing a routing appliance or physical box in a branch location. Some SD-WAN solutions provide additional security capabilities like antivirus services or web content inspection. And in certain instances, the solution is even offered by the Telecom carrier as part of a monthly managed service.)

"Who" is as important as "what" when it comes to SD-WAN DEPLOYMENT?

It's important that additional risk is not introduced when rolling out SD-WANs. Therefore, it matters if you're using an experienced managed service provider than understands the security of your network and will take the time to understand your needs, versus using a Telcom provider. Keep in mind that an inexperienced operator may install SD-WAN routing devices behind a next-gen firewall or Unified Threat Management (UTM) appliance, and bypass the firewall that's already in place for some or all traffic. This would be a major security vulnerability because it could expose the internal networks to public access, bypassing all malware inspection at the UTM.

In addition, the security capabilities offered with the SD-WAN may offer a false sense of security for customers. Does the solution only rely on simple signature-based detections to find malware passing through the network? Advanced and evasive threats can easily circumvent basic antivirus solutions. This is why it's critical to have layered, advanced security services like behavioral-based and artificial intelligence-enabled antivirus as a part of the overall SD-WAN solution deployed at remote sites. Managed SD-WAN solutions may claim to offer some basic firewall services, but they can also take days to respond to simple requests to implement or change basic rules. For example, if an application no longer needs to have a port open, a company should be able to immediately implement a change that no longer exposes it.

Consider looking at new SD-WAN functionality in UTM appliances

If you're already running a next-generation firewall and/or a UTM appliance in your network, consider leveraging the SD-WAN capabilities on those devices to streamline and consolidate functionality. This is often a better approach than relying on new SD-WAN providers that lack security expertise. You may be surprised at the rich functionality that's been added in the last 12 months from security vendors.

About the Author

Brendan Patterson is a Director of Product Management at WatchGuard Technologies, with responsibility for the Fireware operating system, security services, and more. A Certified Information Systems Security Professional (CISSP) Brendan has more than 15 years of experience working with security and networking technologies. Prior to WatchGuard, Brendan was Vice President of Marketing and Product Management at The PowerTech Group, the leader in enterprise security solutions for IBM mid-range servers. Brendan has a master's degree in the Management of Technology from the Massachusetts Institute of Technology, Cambridge, Mass., and a bachelor's degree in mechanical engineering from the National University of Ireland.

Is Your Encryption Flexible Enough?

Introducing the XOTIC™ Crypto System

By Richard Blech, CEO, Secure Channels Inc.

Introduction

The science of modern cryptography utilizes mathematics as the basis for transforming information into an encoded secret that cannot be decoded or translated without the correct key. Encryption techniques are an essential cornerstone in the field of information security, whereby individuals, corporations, and governments wish to protect information and secure it from falling into the wrong hands.

In the United States, the National Security Agency (NSA) has established strict standards for encryption. Today, block ciphers such as the Advanced Encryption Standard (AES), stream ciphers like RC4, and cryptographic hashing algorithms including SHA-256 are utilized worldwide as the basis for protecting everything from banking, to medical records, to very 'private' messages on social media's What's App.

You may be surprised to know that the AES standard was established all the way back in 2001 and set as the US Government standard in 2002. As recently as 2016, significant progress was made in efficiently attacking versions of AES; however, few new standards have emerged since. Most of the world is still working from the same set of security tools that are approaching their 20th birthday.

So, if powerful standardized encryption methods have been easily available and essentially free to the public for decades, then why are there still so many hacks and data breaches that seem to be happening on a regular basis?

There are answers to this question:

Encryption can be extremely difficult to use effectively.

Encryption can be extremely difficult to use effectively. If someone pressured you to hurry up and encrypt something right now, what would be the first tool that you reach for? If you were charged with protecting

an entire enterprise or organization, then what? If you're like many others, these questions could make you stop and think for more than just a few moments. It takes a significant degree of technical expertise and knowhow in order to effectively integrate encryption into regular business operations and workflows.

Ciphers are generally rigid and single-purpose-driven.

Ciphers are generally rigid within their specified modes of operation and could be characterized as purpose-driven. For example, there is a reason that Daniel J Bernstein gained significant acclaim on the worldwide academic stage with his introduction of ChaCha20 and Salsa family of XOR-based streaming ciphers. Simply stated, the AES standard (in its various modes of operations) and other block-ciphers like it are far less performant when it comes to handling streaming media. Why else would it have captured the attention of big players like Google? At the same time, hardware performance boosts available to the AES family of ciphers propel it ahead of ChaCha20 when it comes to large datasets and file-based encryption. AES encryption benefits massively from the inline hardware acceleration that are now commonly included in most Intel Chips. In other words, one flavor of encryption does not fit all applications.

What if you could have it both ways?

What if you could have it both ways? In 2019 Secure Channels Inc. launched the ground-breaking XOTIC™ cryptosystem; a hybridized streaming / block cipher with a "dialable" (user configurable) encryption strength. With less than 1millisecond initialization time, XOTIC is more than 99% faster than AES-256 when encrypting small to modestly-sized data, and blazes past ChaCha20 when encrypting streaming media. XOTIC operates at a minimum of 512bit strength and can be easily "dialed-up" to extreme levels, leaving behind all other block cipher encryption algorithms.

Flexibility is an essential aspect and goal in next generation encryption.

Flexibility is an essential aspect of modern computing platforms and XOTIC delivers on that challenge. XOTIC has recently been deployed to the general public as an email encryption plugin for Microsoft Outlook Office 365, a Windows shell-integrated ZIP utility, and an encryption-as-a-service website. It's been embedded into hardware used by the Hollywood film and entertainment industry, as well as into discrete military applications. Later this summer, XOTIC will be deployed and made available for download at the Apple Store in IOS native apps, Google Play for Android. Products scheduled for release in 2019 even include a ground-breaking new streaming video communications platform.

There's really no true privacy without a better encryption model.

Did you know that when you initiate an online chat or video-call with many of today's popular instant-messaging apps, you are actually only establishing standard (mathematically reversible) PKI-based encryption keys once? Many apps do this only at the time an application is started. This begs the question, "how many different people did you chat with while your instant messaging application was open?" Knowing that all of those 'private' conversations are taking place on the same breakable asymmetric cipher leaves us feeling uneasy. This is in part what prompted Secure Channels to deploy XOTIC into streaming chat apps. Faster XOTIC encryption enciphers (and generates new keys) for every individual video frame and audio packet of a high-definition video contained in a streaming online chat conversation, and without any loss in fidelity. The difference in the level of security protection compared

to other chat apps is geometric, and yet the call quality remains just as crisp as if no encryption was happening at all.

So many new possibilities if we start with a next generation XOTIC platform.

Perhaps most exciting, is that new forms of flexible encryption can now be constructed to ride on top of the XOTIC platform, ushering in an entire new generation of possibilities. "Wave Form Encryption" (WFE) has become a patented new methodology for streaming media that leverages the power of the variable strength encryption offered by the XOTIC cipher. Combining rapid key generation with variable strength encryption has enabled the never-before possible – the ability to modulate encryption strength in real-time like a flowing sine wave.

Summary

Technologies like Wave Form Encryption will literally change the way we communicate. Wave Form Encryption has applicability ranging from cellular phone calls, to video-chat, to firewalls, to military / satellite and space applications. Why would we leave the protection of modern data to a single static cipher from 2001?

Conclusion

The future of encryption technology is here. The key to its success will be packaging it in ways that are easier and more accessible for consumers and businesses alike. The ability to wield stronger and faster encryption technology without complexity will propel the market in the next decade. Providing this type of access via multiple "Secure Channels" is our mission.

For more information on Secure Channels, please visit our website at www.securechannels.com.

About the Author

Richard Blech, CEO of Secure Channels Inc. Richard Blech is an entrepreneur, investor and innovator. His primary business focus is on data security, technology and strategic alliances. As managing member of Imperium Management LLC, Richard actively invests in technologically advanced ventures. He has a discerning ability to determine market trends that are not only lucrative, but also pave the way to technological advancement across the globe. As a resolute advocate of disruptive technology, Richard Blech holds vested interests in cyber-defense and digital content. With cyber-crime breaches now reaching epidemic proportions, Richard's objective is to turn the ever evolving digital world into a risk adverse space that allows everyone to function securely within their ecosystems. As CEO of Secure Channels, Inc., Richard is leading the company to be a leader in enterprise data protection through the development of innovative encryption and authentication based technology solutions. Richard can be reached online at (contact@securechannels.com, @RichardBlech, https://www.linkedin.com/in/richardjblech/) and at our company website http://www.securechannels.com/

The Critical Role TAPs Play in Network Security and Resiliency

By Alastair Hartrup, CEO, Network Critical

Networks continue to be under persistent attack. As a matter of fact, according to CyberEdge's 2019 Cyberthreat Defense Report, the percentage of organizations breached in the past year increased to 78 percent year-over-year. Worse, 32 percent of businesses reported being breached more than 6 times in the last 12 months, up from 27 percent in the previous year.

These attacks take many forms including phishing, ransomware, trojans, DDoS and other destructive malware. And, the motivations for these attacks are as disparate as the threats themselves. Bad actors are perpetrating attacks for financial gain, political influence, competitive advantage and sometimes just to rage against the system. Whatever the motivation, hacking is a significant problem that's impacting productivity and costing organizations billions of dollars every year. Despite all of this troubling news, progress is being made to combat network attacks.

The growth in criminal attacks on networks is paralleled by significant growth and technological advances in the cybersecurity appliance industry. There are many specialized network tools that help reduce the threat landscape by identifying and blocking attacks. For example, Data Loss Protection solutions, Next Generation Firewalls and Unified Threat Management Appliances, Network Analytics platforms, ID and Encryption appliances, and more. In addition, AI and machine learning technologies are making advances in processing millions of security events, new predictive analysis technologies are identifying known threats, and advanced network monitoring appliances are providing traffic flow visibility and analysis.

But ensuring visibility is becoming more challenging as networks move away from centralized architectures. Cloud, hybrid-cloud and remotely hosted applications are driving new types of business activity. Interconnection between users and the remotely hosted information they seek requires multiple links to the internet, corporate intranets, data centers and cloud carriers. It's no longer economically feasible to attach every security appliance directly to every single network link.

Furthermore, when multiple appliances are directly connected to a link it impacts the reliability and availability of the network. Each appliance represents a potential failure point. If the appliance has to be taken offline for maintenance or updates, the link needs to be taken down as well. For example, one unit with a reliability factor of .999 on a link will be down for about 8 hours per year. However, when three units with a .999 reliability factor are deployed on the same link, the overall reliability impact on the link degrades to .997, or about 26 hours per year. As more specialty appliances are added, the overall reliability continues to degrade. Managing these maintenance windows can become a real nightmare.

Network TAPs (Test Access Point) play a vital role in solving these availability and reliability issues. As devices that connect network security and monitoring appliances to network links safely and securely, TAPs receive the network traffic flow. A mirror copy of the traffic is then passed on to an appliance that is also connected to ports on the TAP. While the mirror traffic is passed to the appliance, live network traffic continues to pass back into the network without significant delay. TAPs also provide network fail-safe technology that keeps network traffic flowing even if power to the TAP or connected appliance is lost. Therefore, multiple security appliances can safely be connected to links using TAPs, without impacting the reliability or availability of the live network.

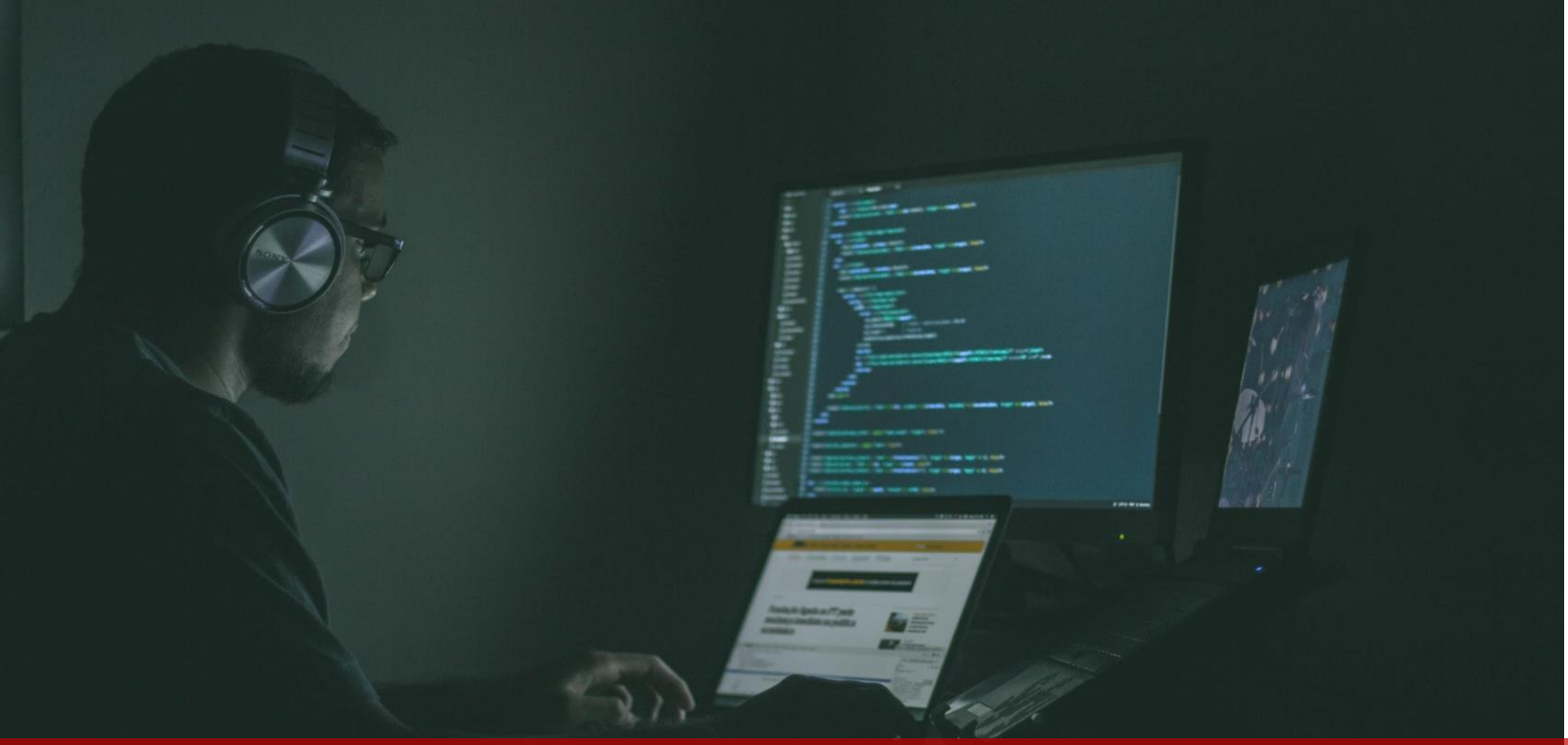
TAPs can be deployed out-of-band or in-line. Monitoring appliances generally use out-of-band mode which, as noted above, sends a mirror copy of the data to the appliance for analysis, but does not interact with live data. Deploying TAPs in-line means that live data travels from the TAP through the appliance and then back into the live network. This method allows security appliances to interact in real time with live data, allowing the appliance to immediately isolate and block malware before damage is done to the network. In-line TAPs automatically bypass an appliance if it's taken offline for any reason. This feature keeps live traffic flowing even if an appliance is down, which simplifies maintenance windows and troubleshooting.

There are also intelligent TAPs on the market that offer aggregation, filtering and port mapping. These features provide additional economic efficiencies allowing flexibility in determining traffic flows to the appliances. By aggregating underutilized links, appliances can support multiple links, providing CAPEX savings. Filtering irrelevant traffic also lessens the traffic burden on appliances allowing more efficient operation and faster response times to threats. Port mapping provides a simple method of directing traffic from the TAP to the appliance and back into the network.

When developing a network protection strategy, it's important to deploy the right monitoring tools and security appliances. Properly including network TAPs in the architecture plan from the beginning is critical to that success. Appliance connectivity with TAPs will allow maximum protection and budget discipline without compromising network reliability or availability.

About the Author

Alastair Hartrup is the CEO and founder of Network Critical, a company that provides industry-leading network TAPs and Packet Brokers, which help organizations increase visibility across dynamic and complex networks. He founded Network Critical in 1997, and today more than 5,000 companies worldwide rely on its technology to help power the network and security monitoring tools needed to control changing infrastructure.



The Hottest Career on the Block

By Nick Galov

Our world is changing fast. Thirty years ago, you left school, choose a potential career path, and worked towards earning the appropriate qualification. You'd then find work and advance along a somewhat linear career path.

Today's school-leavers don't have quite such a clear-cut path open to them. With technological advances changing every aspect of our lives and several traditional industries being completely disrupted, you have to choose a career path carefully or find yourself obsolete.

Advances in artificial intelligence are making automation a much more affordable solution for many businesses. It's a great step forward for businesses, but it also means that the work environment is changing significantly.

Cybersecurity Could be the Answer

With our ever-increasing reliance on tech and AI, one career path shows particular promise. As long as there are cybercriminals out there, there will be skilled people to guard against their attacks.

Cybercrime is a growth industry at the moment. According to TechJury, losses attributed to cybercrime have almost doubled between 2013 and 2017. In 2017 alone, there were 301,580 attacks reported. We shudder to think how many went unnoticed or unreported.

Thanks to these attacks, the demand for experts in the cybersecurity field has never been higher. In fact, there is a global shortage of skilled cybersecurity experts in all levels of the industry. That's a shortage that's not going away any time soon.

According to the United States Department of Labor Statistics, this field is projected to grow by 28% by 2026.

That's a lot faster than most other industries and shows that there is real scope for advancement in this area.

What Positions are We Looking At?

The range of positions within the industry is pretty diverse. What it boils down to, though, is a matter of both training and experience. You'll have to start learning how to protect systems against attacks. The Certified Information Systems Security Professional qualification is the best place to start.

Once you've got the basics under your belt, you can decide what area you'd like to specialize in. The jobs range from an entry-level analyst to engineer or systems architect. Companies require a blend of qualifications and experience. This is not an area where companies are keen on letting employees learn on the job.

That means that getting that first job may be tough. Most companies want at least a year's experience in the industry. Do anything to get your foot in the door, and you're set. Once you start racking up some serious experience and show that you have a talent in this area, you'll be able to write your own ticket.

How Much Scope is there for Advancement?

That's going to be determined by how good you are. If you've got a keen eye for detail and are strong with strategic thinking, then there are a lot of options for you.

You could, for example, follow a more traditional career path, progressing up the ladder as your skills advance. Alternatively, you could start your own security consulting firm and provide advice to companies on improving their systems and security.

Alternatively, you could opt to train the new generation of cybersecurity experts. There are a lot of different options in this field, so it's one that allows for constant growth.

Final Notes

Cybersecurity is one of the hottest fields right now. It's also one that allows you to make a real difference in the world – cybercrime can have devastating consequences for people, and you could help to keep them and their businesses safe.

It's an interesting career as every day is likely to produce new challenges. If you're looking for a career that is interesting and has plenty of scope for advancement, then this is the hottest option right now.

Author the Author

Nick Galov, Hosting Expert and Content Manager. Nick is on a mission to improve the world of web hosting for some time now. When he got the chance to contribute to the betterment of all kinds of software, he simply couldn't say no. When not geeking it out, he enjoys lager and football.

Why CIOs/CISO's Positions Are Becoming More Challenging

By Gamal Emara, Country Manager - UAE at Aruba, a Hewlett Packard Enterprise company

It's your worst possible nightmare. A hacker has breached the company's network and shut down its operations. Millions in revenue is being lost. And the even worse part – you're blamed.

This is becoming an all too familiar scenario for CIOs and CISOs tasked with securing their companies' networks. No sooner have they entered an organisation and put security systems in place, then they find themselves blamed for a successful breach of the company. So, where does it all go wrong?

Network visibility is not a nice-to-have

Most CIOs or CISOs allocate their funding towards securing their data centre. However, when it comes to implementing a system that provides them with full visibility of their network, they consider it simply a nice-to-have.

So they implement basic security elements like a firewall and assume they'll be OK. But, in reality, should an attack happen at the edge of the company's network, they only way they can possibly know is by doing a deep dive to investigate each and every occurrence that might indicate a breach.

We all know this simply isn't possible though. When a user is locked out of their account, the IT department will rarely ever take the time to investigate why. They simply unlock the account and move on to the next problem.

It's true that when a user is locked out, it might be because they forgot their password, but it could also be an indication of something far more sinister.

Every lock-out is a potential attack

Aruba recently had a case, for example, where a client kept on getting locked out of their system. Not realising there was a problem, they kept unlocking the system and moving on. That is until one Sunday morning when around 1000 lock-outs occurred simultaneously. On taking the matter up we discovered that these lock-outs were a direct result of hackers attacking the network in order to access sensitive information.

And, the most concerning part of all this was that the devices being used to launch the attacks were, in fact, the company's own devices. When we investigated further, we found that these devices had actually been stolen some time ago.

Your greatest vulnerability is unguarded

So while CIOs essentially have no idea if and when attacks are happening at the edge, this is exactly where an organisation's greatest vulnerability lies. Think of the average digital environment today – thanks to IoT, there are more connected devices than there have ever been before.

Each device is a potential gateway for a major breach. And think of the consequences of the massive data breaches which have been occurring across the world. Millions are being lost on a regular basis.

One only needs to take a look at the statistics to see the odds of escaping one of these attacks are not good. In fact, according to the 2016 Global Megatrends in Cybersecurity report, 67% of companies with critical infrastructure suffered at least one attack during the course of those 12 months.

How can CIOs and CIS's secure their positions?

The only way a business can possibly remain secure under these circumstances is if the CISO or security team receives notifications as soon as something occurs on the network that is deemed to be out-of-the-norm.

Essentially an end-to-end system that can detect attacks and respond rapidly is vital. And it needs to cover the entire network from the data centre to the edge.

A combination of a network access control solution that is device agnostic, and covers everything from a company's vending machine to industrial IoT equipment, combined with an analytics solution that sits on top of a company's security solutions, for example its firewall. Based on its analyses of these security solutions, the analytics technology creates profiles for individual users. Then if activity takes place on the network which is outside of a user's typical profile, it immediately alerts the security officer.

Say for example, a particular user typically logs into the company network from UAE between 08h00 and 22h00, but then one day that user logs in from Russia at 02h00, the analytics solution will immediately know something is wrong. And it can take this analysis as far as detecting when a user is typing more

slowly to how they would normally. Then once the analytics technology identifies a network intruder, the network access control solution automatically kicks them off the network.

Combined, these two technologies effectively ensure CIOs have, not only visibility, but also complete control of their entire network.

It's the only way to truly ensure you aren't the next CIO a network breach sends packing.

About the Author

Gamal Emara is Country Manager for UAE at Aruba and his role is to grow market share and revenues with partners, alliances and associates, strengthening Aruba's position in the region.

Gamal can be reached online at gamal.emara@hpe.com and at our company website https://www.arubanetworks.com/

The Attribution Problem – Using PAI to Improve Actor Attribution

By Brian Pate, SVP, Babel Street

Within the cyber community, conventional wisdom is that malicious actors can carry out attacks while hiding their true identities. Historically, analysts and investigators have predominantly focused attribution efforts on technical attack aspects, such as digital forensics, malware analysis and signature analysis. That we've yet to fully develop our capabilities or focus efforts at the persona level makes sense, given the technical backgrounds of analysts, traditional reliance on technical indicators of compromise and the difficulty of analyzing the volume of publicly available information. But by applying advanced tools and analysis to publicly available information (PAI), including deep and dark web data, we can begin to deny malicious actors the cloak of anonymity. Moreover, as sophisticated actors increasingly "live off the land," repurpose commodity malware, and use cloud infrastructure to continuously change IP addresses, we're seeing a diminution of the efficacy of technically-focused attribution. Therefore, it's imperative that we build up our PAI capabilities now.

What is attribution?

Broadly speaking, the objective of attribution is to move from an attack's technical observables or related digital personas to the true identity of an individual malicious actor, or actors, whether they be nation state-sponsored actors, ideologic actors or criminals. But while the ultimate objective is a real name and location with a high degree of confidence, it's useful to think of attribution along a spectrum of confidence, with confidence increasing as we gather identifiers that can be used to gain valuable insights about the threat.

At a basic level, PAI analysis finds and links known attack indicators, uncovers unknown indicators, and can yield location, online handles and email addresses, offline aliases and affiliations. These, in turn, can often be linked to quasi-identifiers (QIDs) such as gender, age and date of birth, contained in social-media metadata. Taken individually, none of these indicators are likely to return an identity with a high degree of confidence. But as operators unearth and analyze more leads from PAI sources, each identifier becomes a valuable marker on the road to attribution.

Over time, as operators compile multiple layers of PAI analysis, confidence in the attribution grows, as does the ability to develop insights that come from advanced attribution. Here, operators will begin to discover a malicious actor's associates as well as their aliases. Creating something akin to a social graph, operators can see the context in which a threat operates. That context makes it possible to begin to determine what a malicious actor's current activities might be, as well as their planned activities. Moreover, with context, we can make assessments regarding the malicious actor's capabilities, skill level, strengths and vulnerabilities. The more context we can create, the greater our degree of confidence.

Why is attribution important?

Anonymity is a tremendous asset for malicious actors because it gives them freedom of maneuver. Hostile nation states and malicious actors can mask their attacks or run false flag operations to discredit competitors. Meanwhile, criminals can steal millions of dollars, secure in the knowledge that they'll never face justice.

By denying malicious actors their anonymity, we gain several advantages. We make it more difficult for state actors to carry out their own attacks or use proxies. Along similar lines, attribution can deny malicious actors the freedom of maneuver they need to operate in cyberspace. In the case of cyber criminals, attribution is the prerequisite to assigning legal liability and, where possible, mounting successful prosecutions.

Attribution, even partial attribution, also provides key operational advantages to the defender. The more you know about a threat, including their identity, the better your ability to mount an effective defense. For example, if you know with a high degree of confidence that a malicious actor has capabilities and interest in developing PHP exploits against e-commerce portals, a defender can target their vulnerability identification efforts, expedite patching and configuration hardening, conduct deliberate scans for breaches, and generally act to mitigate the threat. This improves a CSO's ability to better manage risk and make more informed risk decisions.

By achieving attribution with a high level of confidence, properly authorized organizations can also take proactive countermeasures, where appropriate. One possible countermeasure might be infiltrating a forum to dox the malicious actor, burn their alias, or sow discord within the threat community. Another possible countermeasure might be to carry out a hack of the malicious actor's system to either steal the tools they need to carry out their attack or insert malware in order to destroy or disrupt their system.

Finally, it's important to point out that attribution brings much-needed transparency to the cyber ecosystem. Over time, that transparency can have a deterrent effect on state actors and criminals, forcing them to consider whether carrying out their malicious attacks are worth the price of compromising their

identities. Certainly, some attacks will always be worth the cost for malicious attackers, but by using PAI to deny those malicious actors the certainty of anonymity, we can deter and disrupt attacks at scale.

The problem

While there are myriad methods for attribution, it's useful to think in terms of two general categories. One category begins with a persona search seed, such as an email address, social media handle or username. The second category begins with a technical indicator, such as a code snippet, registry value, IP address or domain name. I'll discuss each separately, but in a real-world scenario, both methods typically work in tandem.

A persona search seed can be a valuable lead for querying a variety of sources. Those sources can run the gamut from the open internet to the deep web, to the dark web. Forums, social media, and news sources can often yield artifacts that further the investigation. Ultimately, each artifact increases the investigator's ability to correlate the information they find, allowing them to drive toward a malicious actor's true identity with a high level of confidence.

Of course, using a persona search seed can feel a lot like looking for a needle in a haystack—or more accurately, multiple needles in seemingly unrelated haystacks. But even the most sophisticated malicious actors are susceptible to unmasking because they frequently must use public-facing personas, such as email addresses, to launch their attacks. Furthermore, while a sophisticated actor may practice strong tradecraft, their associates may not. By building context with PAI, investigators can expose the weakest link in the chain and then exploit that advantage to develop attribution of the primary threat actor. Finally, it's important to note that many malicious actors, especially criminals, practice sloppy tradecraft. In many cases, criminals boast about their exploits, and often times those boasts are made in time-stamped forums that allow investigators to intuit their approximate location, intentions, associations and patterns of life.

Of course, a technical indicator, such as snippets of code, malware, and IP addresses can also be a starting point that leads to attribution. Sometimes, a simple file name might provide an artifact that can be used to run a PAI query. Other times paste bins and further accessible documents that support technical collaboration also contain email addresses or handles that can be used in a PAI query. Increasingly, as malicious actors repurpose commodity malware coupled with novel, public-facing command and control infrastructures, they're more likely to leave artifacts useful for attribution sprinkled throughout the attack framework. With the right tools and methods, analysist's can follow these technical leads to improve attribution.

Whether used separately or in tandem, both approaches can provide valuable starting points for PAI inquiries. In time, as investigators assemble more artifacts and build a context around their targets, pulling

QIDs from associated metadata, the inquiry can reveal the location, associates, aliases, and true identities of malicious actors. Just as important, artifacts can also provide insight into past, present and future activities.

Use case #1: Oleksandr Ieremenko

In 2016, the U.S. Department of Justice secured a guilty plea from a New Jersey man who was part of a complex insider trading scheme that exploited confidential information stolen from three separate business news wire services. Prosecutors alleged that the scheme netted tens of millions in illegal profits. The indictment also identified the still-at-large technical mastermind who hacked into the business wires—a Ukrainian citizen named Oleksandr Ieremenko

Mining the indictment for names, email addresses, online handles and other identifiers, we were able to run a series of PAI queries just on Ieremenko. Obviously, we already had a true identity to go on, but the query was fruitful for several reasons. First, we learned a lot about Ieremenko's associates. While these malicious actors weren't indicted, learning who they were and where they operated gave us a better context for understanding the types of malware and tools Ieremenko typically sought to secure. In turn, that information turned up a lot of useful information about Ieremenko's skills, capabilities and past targets. We were even able to assess, with a high degree of confidence, what sorts of targets and schemes Ieremenko was working on before, during and after the indictment.

Use case #2: The Iranian Professor

Using an email address associated with a spear-phishing campaign, we ran a PAI query. As it turned out, this hacker employed sloppy tradecraft by failing to more fully obfuscate QIDs associated with the creation of the email address. While sloppy tradecraft may sound like a lucky break, the key point is that hackers are human. They make human mistakes because they're lazy, careless, poorly trained, pressed for time, etc. These mistakes leave behind artifacts that analysts and investigators can exploit.

In any case, our PAI query told us that the hacker was an Iranian professor. With her true identity, we were able to discover her location, associates, and develop information about her activities, past, present and future. Just as important, we were able to reduce the likelihood that we were meant to discover her true identity as part of a false flag operation.

Unfortunately, this hacker hasn't been brought to justice—and likely won't be. Nevertheless, her identity, area of operation, skill-level, and *modus operandi* provides a powerful check on her operations going forward.

Conclusion

Attribution is an important component of full-spectrum cyber operations, and as attribution using purely technical methods becomes more difficult, we should improve our ability to use PAI to further the objectives of advanced attribution. While there is no single, silver-bullet solution for ending malicious cyber activity, by making life more difficult for malicious actors, we can more easily disrupt and deter the threats they pose. Just as important, as we learn the names of malicious hackers around the world and increase what we know about them, we shine a light into cyberspace that makes it easier to parse the signal from the noise. Knowing who poses the threat, where they're attacking from, what they intend to do, and the extent of their capabilities can boost our defenses and countermeasures immediately, and in the long run, inform the framework we need to build to address a range of threats.

About the Author

Brian currently serves as the SVP for Babel Street's Federal Civil business, where he is responsible for Babel Street customer engagements spanning the Executive and Legislative Branches, to include the Departments of Justice, State and Homeland Security. Prior to this position, Brian served as the Current Operations officer at Marine Forces Cyberspace Command and Global Plans lead at Joint Task Force Ares, where he was responsible for planning and executing full spectrum, global cyberspace operations. In this capacity, he also ran several 24/7 operations centers responsible for crisis planning and crisis response. Brian is a graduate of Georgetown University's School of Foreign Service and several advanced military courses. He is a member of the SANS GIAC Advisory Board and a board member of the Capitol Hill Community Foundation.


EVENTS

C-SUITE & SENIOR LEVEL EXECUTIVES ONLY

CYBER SECURITY SUMMIT 2019

PROTECT YOUR BUSINESS FROM CYBER ATTACKS

$150 ADMISSION | Use Promo Code: **CDM19** for $150 Admission.
(Standard Admission: $350)

Register Now at **CyberSummitUSA.com** »

6 CPE CREDITS Full day attendance earns 6 credits following the Summit

2019 CYBER SECURITY SUMMITS

Denver, CO - Apr. 2	**DC Metro, VA** - Jul. 16	**Scottsdale, AZ** - Oct. 17
Philadelphia, PA - Apr. 25	**Chicago, IL** - Aug. 27	**Boston, MA** - Nov. 6
Dallas, TX - May 16	**Charlotte, NC** - Sep. 17	**Houston, TX** - Nov. 21
Seattle, WA - June 25	**New York, NY** - Oct. 3	**Los Angeles, CA** - Dec. 5

THOUGHT LEADERS INCLUDE

Bryan Deyoung
Digital Forensics Lab Philadelphia
U.S. Secret Service

Deb Walter
Manager InfoSec Policy, Standards, Training & Awareness
AmerisourceBergen

Ryan Spelman
Senior Director
Center for Internet Security

Paul De Souza
Founder & President
Cyber Security Forum Initiative

Tory Smith
Special Agent
The FBI

This Pass is for C-Suite & Sr. Level Executives only and includes a Catered Breakfast, Lunch & Cocktail Reception. Sales/Marketing professionals will Not admitted.

INTERACTIVE PANELS

RANSOMWARE
To Pay or Not To Pay - That is the Question!

INSIDER THREAT
Protect Your Enterprise from the Human Element

ORCHESTRATION
CISO & Sr. Leadership's Best Approach to Cyber Defense

CLOUD INSECURITY
Common Pitfalls that Organizations Make when Moving to the Cloud and How to Avoid

INCIDENT RESPONSE
What to do Before, During and After a Breach

To Speak or Exhibit at a future Summit, contact:
MHutton@CyberSummitUSA.com

CYBER SECURITY & CLOUD EXPO WORLD SERIES

EXPLORING THE SECURITY NEEDS OF FUTURE TECHNOLOGY

GLOBAL
25-26 APRIL 2019
OLYMPIA GRAND, LONDON

EUROPE
19-20 JUNE 2019
RAI, AMSTERDAM

N.AMERICA
NOVEMBER 13-14, 2019
SANTA CLARA, CA

TOPICS INCLUDE

- Data Intelligence
- Ecosystem
- Security
- Enterprise
- Privacy
- Governance
- Identity
- Infrastructure

REGISTER NOW FOR FREE

+44 (0) 117 980 9020 | enquiries@cybersecuritycloudexpo.com | www.cybersecuritycloudexpo.com

Co-hosted Events

BLOCKCHAIN EXPO WORLD SERIES

AI & BIG DATA EXPO WORLD SERIES

IoT TECH EXPO WORLD SERIES

Limited Group Discounts for 3 or more! Reserve Your Seats Now!

5 Exclusive Expert-Led Workshops are Available!
(Contact us for more details)

3rd CYBER SECURITY FOR AIRPORTS SUMMIT 2019

- Main Summit: **19 & 20 June 2019**
- Workshops: **18 & 21 June 2019**
- Venue: **Singapore**

Premier Networking and Learning Platform to Discuss and Hear Best Practices on Improving Airport Cyber Security Measures to Prevent Cyber Attacks!

A MUST ATTEND SUMMIT IN 2019

Comprehensive Case Studies
Gain strategic insights from industry experts on how they overcome major Cyber Security Challenges at their airports

Latest Trends in Cyber Security
Exposure to the latest Cyber Security Measures, Comprehensive Cyber Solutions & Developments in Cyber Security Technology

Best Practices to Increase Cyber Readiness
Get interactive with global airport authorities in panel discussions and 6 comprehensive summit workshops for in-depth discussions

Interactive Workshops
Get interactive with global airport authorities in 5 comprehensive summit workshops for in-depth discussions and knowledge sharing

Researched & Developed By: EQUIP GLOBAL

CONTACT US TODAY!

PHONE +65 6376 0809 **EMAIL** enquiry@equip-global.com
WEBSITE https://www.equip-global.com/3rd-cyber-security-for-airports-summit

The only big data conference designed specifically for the defence sector

Defence iQ a division of IQPC presents

BIG DATA FOR DEFENCE

Conference Days: 26-27 June 2019
Pre-Conference Workshop: 25 June 2019
Hilton London Olympia, London, United Kingdom

Realising the Military Utility of Big Data

Our international Big Data for Defence speaker panel includes:

Dr. David Horner, Director, Information Technology Laboratory Modernisation Program, **U.S. Army Engineer Research and Development Center**

Brigadier General Jennifer Buckner, Commander, **Cyberspace Operations Directorate**

Lars Findsen, Director, **Danish Defence Intelligence Service**

Air Commodore Tim Neal-Hopes, Deputy Head of Cyber Policy / Joint User for Cyber, **UK Ministry of Defence**

Colonel Jerome Lemaire, Head of Digital, Defense Systems and Integration of Artificial Intelligence, **Directorate General of Armaments, French Ministry of Defence**

Auke Venema, Principal Member, NATO Science and Technology Board, **Netherlands Ministry of Defence, NATO**

Attend Big Data for Defence to:

"The conference provided very good validation of EU and NATO market changes"
Norm Balchunas, Senior Director, Honeywell

- Understand how to **securely store and rapidly analyse** data using the latest systems to **generate actionable intelligence**
- Receive in-depth updates on big data procurement programmes, including the French **ARTEMIS project**, and how artificial intelligence and big data can combine to generate the capability
- **Identify partnership opportunities** with traditional and non-traditional defence entities offering key solutions for big data analytics and artificial intelligence
- Gain a fundamental understanding of big data, terminologies in use and it's **application in defence**

Sponsors: Honeywell THE POWER OF CONNECTED, MarkLogic

Partners: Team Defence Information www.teamdefence.info, Warfare.Today, CDM Cyber Defense Magazine

TO REGISTER: +44 (0) 207 036 1300 | ENQUIRE@DEFENCEIQ.COM | BIGDATADEFENCE.IQPC.COM

GCC FORENSICS
CONFERENCE & EXHIBITION

13 - 14 NOV 2019 | THE GULF HOTEL BAHRAIN

مؤتمر ومعرض الخليج العربي للأدلة الجنائية

THE MUST ATTEND EVENT FOR THE ENTIRE FORENSIC SECTOR IN THE MIDDLE EAST

LAW ENFORCEMENT FORENSICS
FORENSIC LABS | INVESTIGATIONS/RESEARCH
DIGITAL FORENSICS | ACADEMIA
COURT ROOMS AND CRIMINAL LAW | SECURITY

13 - 14 November 2019

www.gccforensics.com

/gccforensic

@gccforensic

@gccforensic

Media Partner

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Supported by

Ministry of Interior

Organised by

CLARION EVENTS

UNDER THE PATRONAGE OF HIS MAJESTY KING HAMAD BIN ISA AL KHALIFA, KING OF THE KINGDOM OF BAHRAIN

WINNER
BEST TRADE SHOW OVER 10,000SQM IN THE MIDDLE EAST
MESE 2018 AWARDS

معرض ومؤتمر البحرين الدولي للدفاع
BIDEC
Bahrain International Defence Exhibition & Conference

BAHRAIN'S PREMIER INTERNATIONAL TRI-SERVICE DEFENCE SHOW

28 - 30 October 2019
Bahrain International Exhibition & Convention Centre

Over 9,000 visitors from **49 countries**

180 + Exhibiting Companies

5 Off-Site Activities + Strategic Military Conference

Fully-Hosted VIP Delegation Programme

www.bahraindefence.com /visitbidec @visitbidec @visitbidec2019

Gold Sponsor

LOCKHEED MARTIN

Officially Supported by

Bahrain Defence Force
Royal Bahrain Air Force
Royal Guard
Royal Bahrain Naval Force
National Guard
Ministry of Foreign Affairs
Ministry of Information Affairs

Media Partner

CDM CYBER DEFENSE MAGAZINE

In Conjunction with

MEMAC
Middle East Military Alliances & Coalitions

Knowledge Partner

DERASAT

Organised by

FAALIYAT MANAGEMENT CO. W.L.L.

CLARION EVENTS

HELD UNDER THE PATRONAGE OF HIS EXCELLENCY, PRESIDENT ABDEL FATTAH EL-SISI
THE PRESIDENT OF THE ARAB REPUBLIC OF EGYPT, THE SUPREME COMMANDER OF THE EGYPTIAN ARMED FORCES

EGYPT DEFENCE EXPO

7-10 DECEMBER 2020
EGYPT INTERNATIONAL EXHIBITION CENTRE

www.egyptdefenceexpo.com
@egyptdefenceexpo
/egyptdefenceexpo
@visitedex
#edex2020

THE 2ND EDITION OF EGYPT'S ONLY INTERNATIONAL DEFENCE EXHIBITION

EGYPT INTERNATIONAL EXHIBITION CENTRE
7-10 DECEMBER 2020

400 + EXHIBITORS

30,000 + VISITORS

FULLY-HOSTED VIP DELEGATION PROGRAMME

Media Partner

CDM
CYBER DEFENSE MAGAZINE

Supported by

Ministry of Defence

Egyptian Armed Forces

Ministry of Military Production

Organised by

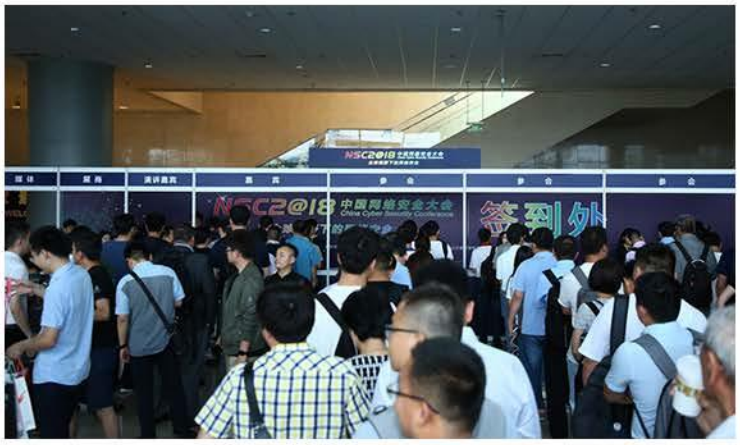
CLARION EVENTS

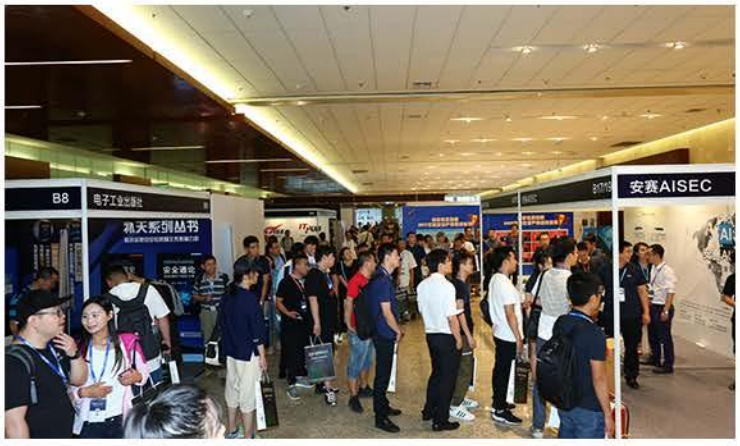
China Cyber Security Conference & Exposition 2019

Beijing 13th June 2019

China Cyber Security Conference & Exposition 2019 (NSC 2019) is the leading information security event in China which has been successfully held for six years since 2013. It will attract more than 3,000 information professionals from government, private sector, academia and 80+ media outlets. Carrying the theme of 'Globalization of Cyber Security', the Conference and Expo will address the most up-to-date security and cyber security issues; from the latest trends, risks, strategies, technologies, including case studies and solutions. It has become a well-known and important exchange platform for information security professionals from China and the rest of the world.

Join us for the engaging sessions and intense networking. Get exposure to innovative technologies, solutions, and leadership that will help secure our digital world.





Official Website: http://nsc.skdlabs.com/en

2019 CYBER INVESTING SUMMIT™

EXPLORE THE FINANCIAL OPPORTUNITIES AND STRATEGIES AVAILABLE IN THE CYBERSECURITY SECTOR

MAY 16TH, 2019 | NEW YORK

10% OFF ADMISSION CODE CDMCYVEST19

CYBERINVESTINGSUMMIT.COM

Defence iQ
a division of IQPC

*The world's **only** countering drones conference dedicated to the security community*

COUNTERING DRONES

Detect, Identify and Neutralise

Conference: 10th-11th July 2019
Workshop Day: 9th July 2019
Hilton London Olympia, London, UK

"PROBABLY THE BEST CUAS EVENT I HAVE BEEN TO"

John Scott Mathews, Senior Privacy Advisor, Intelligence, U.S. Department of Homeland Security

Leading discussions will be:

Brian Harrell, Assistant Director, Infrastructure Security, U.S. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, **U.S. Government**

Peter Clarke, Director C-UAS, **UK MoD**

Helmut Spahn, Director Security, **FIFA**

Nicolas Marcou, Director, Drone Programmes, **Directorate of Civil Aviation Security (France)**

Dr. Hussain Alhallaf, Security Director, **Riyadh Airports**

Colonel Jean François Morel, Counter UAV Lead, **Gendarmerie Nationale**

5 reasons to attend Countering Drones 2019:

- Gain an understanding of what future drone threats look like and **how to prepare your organisation for them**
- Acquire the knowledge of **how to respond effectively to drone disruption** cooperatively with other organisations and agencies
- Align your current plans with the latest solutions and **recommendations from leading experts**
- Deepen your knowledge of risk and security to understand **how to protect your organisation** more cost-effectively
- Influence future policy and demonstrate thought leadership by **contributing to discussions** with key industry experts

Sponsors: AVEILLANT A Thales company · HENSOLDT Detect and Protect. · RHEINMETALL DEFENCE · robin radar systems

To Register: www.counteringdrones.com • enquire@iqpc.co.uk • +44 (0)20 7036 1300

ICRC
Blavatnik Interdisciplinary Cyber Research Center

Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

מערך הסייבר הלאומי - משרד ראש הממשלה
National Cyber Directorate - Prime Minister Office

סייבר ישראל
Cyber Israel

In cooperation with:
Ministry of Foreign Affairs Israel

Cyber Week

June 23rd-27th, 2019

Tel Aviv University, Israel

Cyber Week 2019, the leading international cyber event, provides exclusive access to key insights from cybersecurity experts and creates a forum for networking and knowledge exchange. Learn best practices firsthand from industry leaders and innovators, and discover what the future holds for cyber.

8000	80	25%	400
Attendees	Countries	Attendees from abroad	Expert speakers

Cyber Leaders Forum | Academic Conference | Cyber Challenge | Blockchain: The New Digital Age | The Future of Artificial Intelligence | Fraud & Cyber Crime | BSides TLV | Rethink Cyber by Team 8 | Policy & Privacy Conference| Startup Day | Security in the Quantum Age | From GDPR to CCPA | Building a Global Network of Cybersecurity Hub's | Cyber Attacks Against Nations | Workshops and Trainings

Visit Cyber Week website to find out more about some of the speakers and events we have planned!
Attendance is free Tel: +972-3-6406041 Email: icrc@tauex.tau.ac.il cyberweek.tau.ac.il

"Asia's Premier Counter-Terrorism and Internal Security Exhibiton and Conference!"

The 2nd Edition of

CTAX

COUNTER TERROR ASIA EXPO 2019

Co-Located With:

CTAC 2019

An International Conference on Counter-Terrorism and Internal Security

Incorporating 3 Major Segments:

HOMELAND SECURITY ASIA 2019

An International Exhibition On Homeland and Border Security Equipment and Technology

ICIDA

INSTALLATION AND CRITICAL INFRASTRUCTURE DEFENCE ASIA 2019

An International Exhibition On Installation And Critical Infrastructure Protection Equipment and Technology

CDA 2019

CYBER DEFENSE ASIA

An International Exhibition On Countering Cyber Terrorism and Cyber Defence.

OCTOBER

16 - 17

Jakarta International Expo Kemayoran, Indonesia

For more info, contact us:

Phone: (+65) 6100 9101

Email: sg@asiafireworks.com

www.counterterrorasia.com

Organized by:

FIREWORKS TRADE MEDIA GROUP

Fireworks Trade Media Pte Ltd

Strategic Partner:

Supporting Organizations :

Media Partners :

Internet of Things World

May 13 - 16, 2019
Santa Clara Convention Center, CA

THE INTERSECTION OF INDUSTRIES AND IOT INNOVATION

12,500+ Attendees

400+ Speakers

300+ Sponsors & Exhibitors

2019 Event Features

- Full Day of Executive Keynotes
- IoT World Awards & Gala Dinner
- Developer Conference
- Hackathon
- Expo Tours
- Networking Parties
- Startup Elevate

2019 CONFIRMED SPEAKERS INCLUDE:

Southwest. **Adi Pradeep**
Cybersecurity Analyst
Southwest Airlines

CITY OF PALO ALTO **Raj Patel**
Chief Information Security Officer
City of Palo Alto

MOCANA **Dean Weber**
CTO
Mocana

9+ DAILY CONFERENCE TRACKS COVERING:

Manufacturing | Smart Buildings & Energy | Smart Cities | Connected Consumer | IoT Security | IoT Connectivity | Supply Chain & Logistics | And more!

SAVE 20% ON YOUR CONFERENCE PASS USING CODE CYBER OR REGISTER FOR YOUR FREE EXPO PASS

Learn more at www.iotworldevent.com

ISDEF
ISRAEL DEFENSE & HLS EXPO
PART OF THE AVNON GROUP

JUNE 4-6
2019
TEL-AVIV ISRAEL

DO YOU OPERATE WITHIN THE CYBER REALM?

SECURE YOUR BOOTH AT ISDEF 2019

- COMPREHENSIVE EXHIBIT OF LATEST TECHNOLOGY
- WORLD RENOWNED KEYNOTE SPEAKERS
- B2B & B2G MATCHMAKING PROGRAM
- PROFESSIONAL WORKSHOPS
- LIVE DEMONSTRATIONS

JOIN US ON JUNE 4 - 6 FOR THE 10TH EDITION OF ISDEF'S DEFENSE, HOMELAND SECURITY & CYBER EXHIBITION!

Showcase your latest solutions, attend exclusive networking events, participate in world class workshops, and take advantage of our unique business matchmaking program. During this 3 day period, ISDEF will present options for your firm to meet with the world's leading defense and homeland security establishments.

ISDEF 2019 anticipates more than 300 exhibitors, 15,000 visitors from more than 90 nations, and 100 high-ranking official delegations from Israel and abroad, making it the ultimate venue for you to market your cyber solutions and services. The exhibition provides a unique opportunity to interact directly with the Israeli and International Homeland Security and Cyber markets on a grand scale.

BUKY CARMELI

Former Director General of the Israeli National Cyber Security Authority, ISDEF's Board of Advisors

"ISDEF is recognized as Israel's largest Defense, HLS & Cyber exhibition since 2007. The exhibition features high ranking government officials in addition to leading decision-makers from both the public and private sectors. ISDEF has proven time and time again as the ultimate platform for Israeli and International cyber firms to receive exposure and recognition from select decision-makers from both domestic and international delegations. In addition, ISDEF's B2B and B2G platform has made it possible for cyber firms to greatly enlarge both their customer base and their profits, as well as expanding brand awareness."

AMONG OUR PREVIOUS EXHIBITORS & SPONSORS IN THE CYBER REALM

TECHFEST · BLER · obility · cybereason · CYCURITY · Dome9 · evigilo · FENROR7 · GATESCANNER · hp · GPS dome · HackingTeam · InteliComm · IntelliSiG · INTSIGHTS · KELAGROUP · Regulus · OCTOPUS · MAGEN · MER Group · CAT · Geektime · mobilecrypto · nowforce · perimeter 81 · PICSIX · SAFE-T · SEG · SMOFS · TACTICAL LABS · TERRASAFE · Terrogence · VERINT · INSS · VOTIRO · ZIMPERIUM · SAFE-ZONE

www.isdefexpo.com

CYBERTECH MIDWEST

JULY 24-25, 2019 // INDIANA CONVENTION CENTER

Together with:

CYBER.

WE LIVE IT. BREATHE IT.

Cybertech Worldwide. Creating Business Opportunities Across Borders.

SAVE THE DATE FOR CYBERTECH MIDWEST 2019!

Join us on July 24-25, 2019, at the Indiana Convention Center in Indianapolis, with leading experts from the world of cyber!

>> **700+** Attendees >> **53+** Speakers
>> **31+** Sponsors and Partners >> Participation from over **20** states

Come **LEARN**, **NETWORK**, and **EXPLORE** the wide range of business opportunities at your disposal with the cyber industry's most prominent players.

Top executives. Government officials. Great business networking opportunities. All at the forefront of global and regional innovation!

Register today at **www.midwest.cybertechconference.com** | More info at **contact@cybertechmidwest.com**

13th ITS EUROPEAN CONGRESS

FULFILLING ITS PROMISES

Brainport Eindhoven, the Netherlands | 3-6 June 2019

Join Europe's biggest event on Intelligent Transport Systems & Services


TCCA
CRITICAL
COMMUNICATIONS
WORLD 2019
REGISTER NOW
SERVING THE CRITICAL COMMUNICATIONS SECTOR
FOR OVER 20 YEARS
@CritCommsSeries
TCCA Critical Communications Series
www.critical-communications-world.com
18th – 20th June
MiTEC, Kuala Lumpur

CYBER SECURITY EXCHANGE Healthcare

May 19-21, 2019
Dallas, Texas

The **Cyber Security for Healthcare Exchange** offers a true peer-to-peer networking forum while highlighting the latest technologies, strategies and processes to improve resilience with talent shortfalls and emerging technologies.

Come join fellow C-level peers from billion dollar plus organizations at this exclusive invitation-only event. In order to foster a more collaborative and intimate networking setting we cap our events at 40 delegate attendees so space is limited. Past event attendees include leaders in Cyber Security from organizations like:

- Aetna
- AmerisourceBergen
- Johns Hopkins
- United Health Group
- Blue Cross Blue Shield
- Kaiser Permanente
- Molina Healthcare
- Stryker
- GE Healthcare
- Humana
- Merck & Co.
- New York Life Insurance
- Envision Healthcare
- Plus many more!

Join this interactive three-day forum in Dallas, where impactful and practical information will provide insights to heads of cyber security within healthcare. The program includes topics like:

- Holistic Threat Management - Minimizing Threats and Increasing Resilience
- Transformational Security – Next Steps for Healthcare
- Cybersecurity Spend: Proactive Stakeholder Communications
- Evolving Threat Hunting: Ransomware, WannaCry, What's Next?
- Privacy & Security of Medical Data: When Everyone Wants to Bring Their Own Device
- Identifying, Monitoring and Mitigating Healthcare Security Risks in the Cloud
- Obtaining Security Resilience in Healthcare
- Plus more!

Contact us today to find how you might join this dynamic, executive-level affair.

cyberhealthcare-exchange.iqpc.com/request-an-invite

5TH ANNUAL

CYBER SECURITY FOR DEFENSE

EXPLORE CYBERSECURITY SOLUTIONS WITH MILITARY AND GOVERNMENT

Meet and Network with:

- **Rear Admiral Danelle Barrett,** Cyber Security Division Director, United States Navy
- **Mitchell Komaroff,** SES, Principal Advisor for Cybersecurity Strategy, Planning & Oversight, DoD CIO
- **Col. Timothy Lawrence,** Director, Information Directorate, and Commander, Detachment 4, AFRL

JUNE 26-28, 2019

WASHINGTON, D.C.

Cybersecurityfordefense.com

idga@idga.org

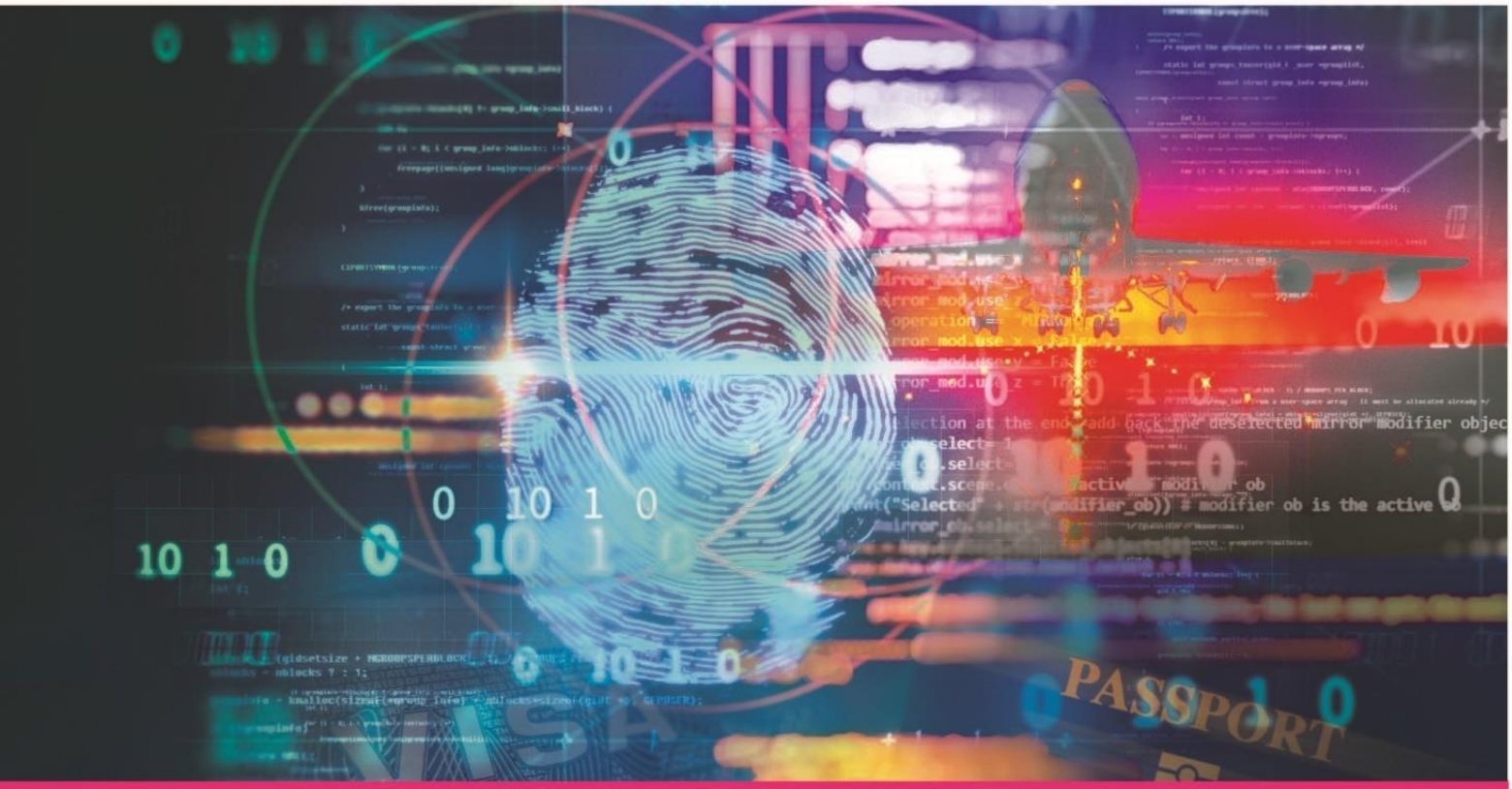
U.S. Military and Government Attend for

FREE

IDENTITY WEEK

GLOBAL • TRUSTED • VISIONARY

SDW2019 | PLANET BIOMETRICS 2019 | DIGITAL:ID 2019



EXPLORING NEXT-GENERATION GOVERNMENT, COMMERCIAL & CITIZEN IDENTITY SOLUTIONS

- Identity Week comprises of three world-class events: Digital:ID, Planet Biometrics and SDW - all focused on the concept of identity.
- At Identity Week 2019 join: **3000+ Event Attendees | 500+ Conference Delegates | 200+ Exhibiting Organizations | 250+ Speakers | 3 Co-located Events | From over 80 countries**

IDENTITY WEEK
3 Days • 3 Exhibitions • 3 Conferences
11-13 June 2019
ExCeL, London, UK

Created by

science media partners

SPARK SOMETHING TERRAPINN

www.terrapinn.com/identityweek


ISAF
IT SECURITY
8TH INTERNATIONAL INFORMATION
& NETWORK SECURITY EXHIBITION
OCTOBER 17TH-20TH, 2019
Istanbul Expo Center (İFM) - Yesilkoy / Istanbul
www.isaffuari.com
MARMARA
TANITIM FUARCILIK
www.marmarafuar.com.tr | Tel: +90 212 503 32 32 | marmara@marmarafuar.com.tr
KOSGEB
BU FUAR 5174 SAYILI KANUN GEREĞİNCE TOBB (TÜRKİYE ODALAR VE BORSALAR BİRLİĞİ) DENETİMİNDE DÜZENLENMEKTEDİR.

#CYBERBYTE
@ROSSOWESQ

Meet Our Publisher: Gary S. Miliefsky, CISSP, fmDHS

“Amazing Keynote”

“Best Speaker on the Hacking Stage”

“Most Entertaining and Engaging”

Gary has been keynoting cyber security events throughout the year. He’s also been a moderator, a panelist and has numerous upcoming events throughout the year.

If you are looking for a cybersecurity expert who can make the difference from a nice event to a stellar conference, look no further email marketing@cyberdefensemagazine.com

CYBER DEFENSE TV

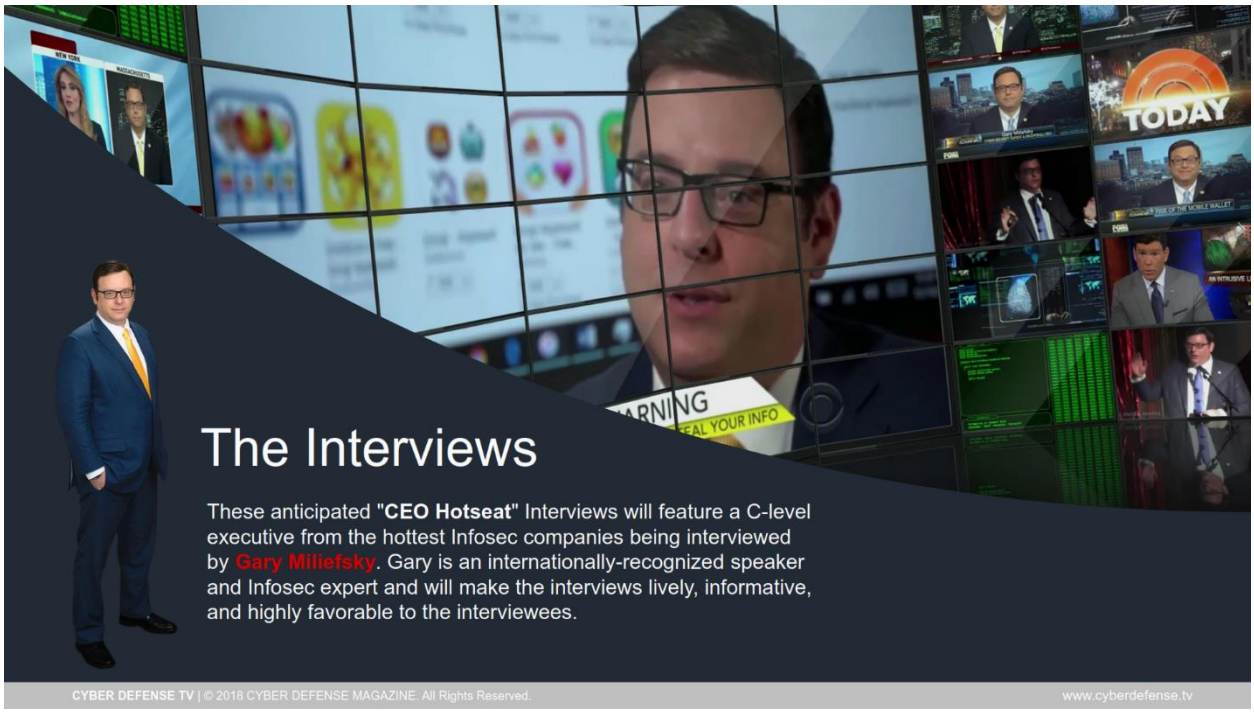
INFOSEC KNOWLEDGE IS POWER

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

At least a dozen exceptional interviews rolling out each month starting this summer…

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.

Marketing and Partnership Opportunities

Banners, E-mails, InfoSec Awards, Downloads, Print Editions and Much More…

Job Opportunities

Send us your list and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

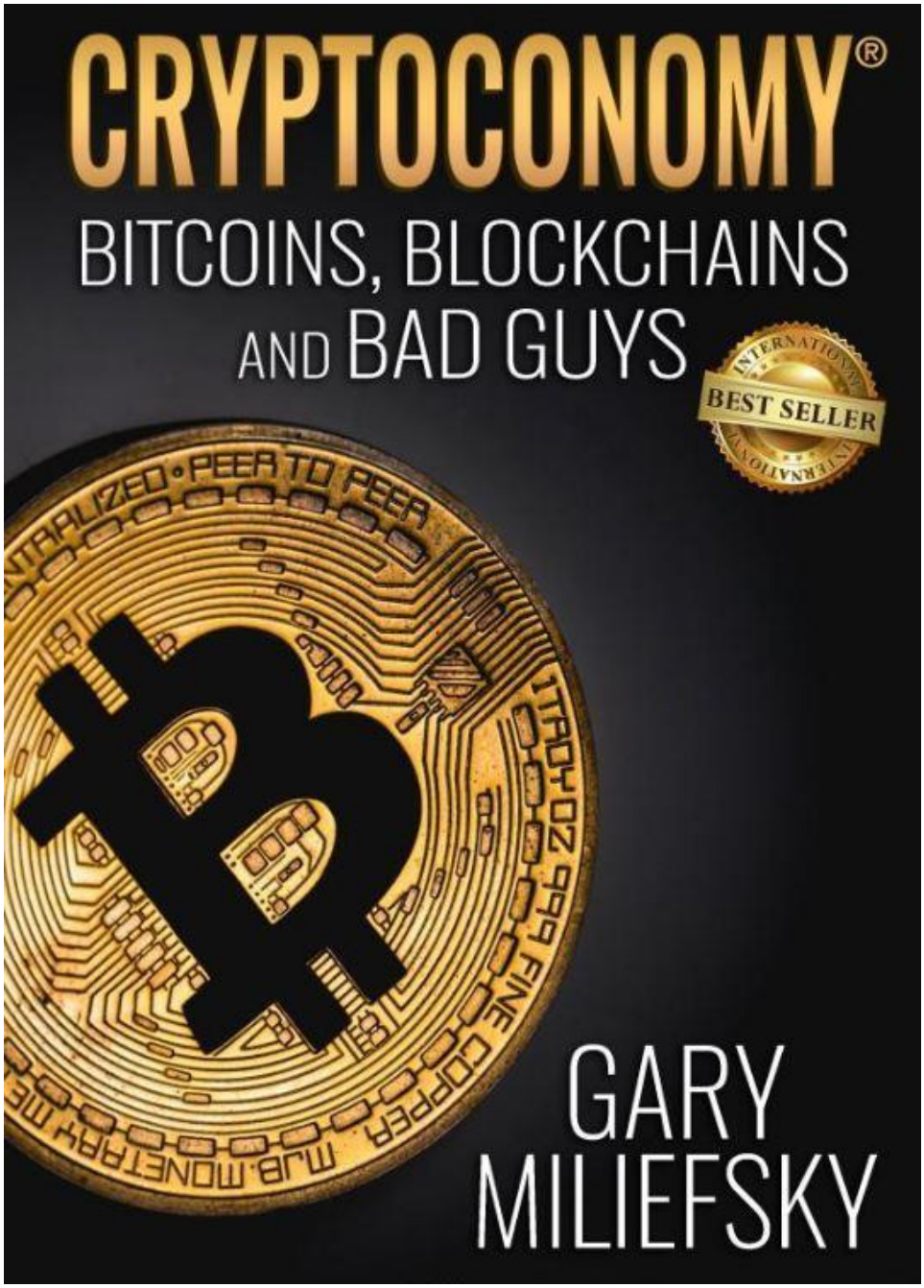
Cyber Defense Magazine

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: 05/01/2019

TRILLIONS ARE AT STAKE

No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES



Pressed for time?

Explore managed file transfer for your organization, instantly!

You need a way to simplify, secure, and automate critical file transfers through a centralized, enterprise-level solution. That's where GoAnywhere comes in.

GoAnywhere MFT is a robust managed file transfer solution for organizations of all sizes. Whether you're in the cloud, on-premises, or operate in a hybrid environment, GoAnywhere has you--and your most critical data--covered in transit and at rest.

If you're short on time and need answers fast, take our feature tour! You'll get a quick overview of the benefits and features GoAnywhere provides, just like that.

Is managed file transfer for you?

Explore our industry-leading MFT solution anytime in this on-demand demonstration: **www.goanywhere.com/watch-a-demo**

GO ANYWHERE®
Managed File Transfer

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

Does Your Organization Need MFT Software?

Determine if a secure file transfer solution is right for your situation.

Managed File Transfer (MFT) solutions improve and streamline critical file transfer processes, including encryption, automation, data security compliance, and trading partner collaboration.

But is this solution right for you?

GO ANYWHERE®
Managed File Transfer

You might benefit from MFT if:

1. You need to audit your file transfer activity.
2. You need to comply with data security laws and regulations.
3. You use traditional methods (e.g. FTP or legacy scripts) to send data.
4. You need to easily and securely exchange data with trading partners.

GoAnywhere MFT is a secure file transfer solution that's quick to implement and user-friendly for all.
See for yourself how MFT can help your organization with these four needs and more. Try a 30-day trial today.

Benefit from MFT Today. Start Your Trial. **www.goanywhere.com/trial**

HERJAVEC GROUP

The sea of connected devices is a dangerous place.
You want a **Shark** on your team.

Top Ranked MSSP & Global Cyber Operations Leader

- ✔ Advisory Services
- ✔ Identity Services
- ✔ Technology Architecture & Implementation
- ✔ 24/7 Managed Security Services
- ✔ Threat Management
- ✔ Incident Response

Robert Herjavec
Star of ABC's Shark Tank
CEO & Founder of Herjavec Group

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNER

- Security Company of the Year
- Identity and MSSP Leader

Black Unicorn Awards 2019

Cyber Defense Media Group Announces Black Unicorn Awards for 2019

Cyber Defense Media Group (CDMG), the industry's leading electronic information security media group, is announcing that the annual Black Unicorn awards are now open. Innovative information security companies of any size, that have not yet gone public, with a public market valuation of $1B USD or more may apply for this prestigious award.

- All Official Nomination Forms must be received by the Judges at nominations(at) blackunicornawards(dot)com no later than June 19, 2019.
- Judging will begin on June 19, 2019 and 30 Finalists will be selected by the Judges on July 9, 2019.
- An announcement of the 30 Finalists will go out on the wire and through CDMG marketing vehicles on July 11, 2019.
- Ten Winners will be selected by the Judges between July 11, 2019 and July 19, 2019.
- Winners will be announced on August 7, 2019 during Black Hat USA 2019. Winners will be featured in the Black Unicorns Annual Report for 2019, released during Black Hat USA 2019.

Judges for these prestigious awards includes cybersecurity industry veterans, trailblazers and market makers Gary Miliefsky of CDMG, Robert Herjavec of Herjavec Group and David DeWalt of NightDragon. Learn more about the judges at: **http://cyberdefenseawards.com/black-unicorn-awards-2019-meet-the-judges/**

Cybersecurity companies that wish to apply may visit **http://www.cyberdefenseawards.com/**

www.cyberdefenseawards.com